ID: 635258
Sample Name: DHL WB# 2343640950.exe
Cookbook: default.jbs
Time: 17:56:26
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report DHL WB# 2343640950.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Memory Dumps 6
Unpacked PEs 6
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 7
AV Detection 7
Networking 7
E-Banking Fraud 7
System Summary 7
Data Obfuscation 7
Hooking and other Techniques for Hiding and Protection 7
Malware Analysis System Evasion 7
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Remote Access Functionality 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 11
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
World Map of Contacted IPs 15
Public IPs 15
General Information 16
Warnings 16
Simulations 16
Behavior and APIs 16
Joe Sandbox View / Context 16
IPs 16
Domains 17
ASNs 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 17
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL WB# 2343640950.exe.log 17
Static File Info 17
General 17
File Icon 18
Static PE Info 18
General 18
Entrypoint Preview 18
Data Directories 20
Sections 20
Resources 20
Imports 20
Version Infos 20
Network Behavior 21
Network Port Distribution 21
TCP Packets 21
UDP Packets 21
DNS Queries 21
DNS Answers 21
HTTP Request Dependency Graph 21
HTTP Packets 22
Code Manipulations 22

User Modules 22
Hook Summary 22
Processes 22
Statistics 22
Behavior 22
System Behavior 23
Analysis Process: DHL WB# 2343640950.exePID: 7048, Parent PID: 2760 23
General 23
File Activities 23
Analysis Process: DHL WB# 2343640950.exePID: 6376, Parent PID: 7048 23
General 23
Analysis Process: DHL WB# 2343640950.exePID: 6380, Parent PID: 7048 24
General 24
File Activities 24
File Read 24
Analysis Process: explorer.exePID: 3688, Parent PID: 6380 25
General 25
File Activities 25
Analysis Process: cmstp.exePID: 7120, Parent PID: 3688 25
General 25
File Activities 26
File Read 26
Analysis Process: cmd.exePID: 4124, Parent PID: 7120 26
General 26
File Activities 26
Analysis Process: conhost.exePID: 3844, Parent PID: 4124 26
General 26
Disassembly 27

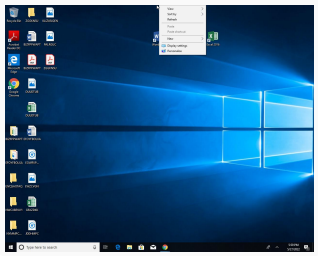
Windows Analysis Report

DHL WB# 2343640950.exe

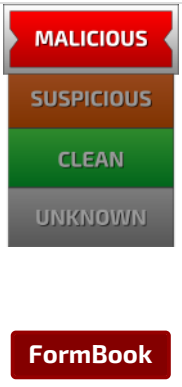
Overview

General Information

Sample Name:	DHL WB# 2343640950.exe
Analysis ID:	635258
MD5:	81e4012e3036be.
SHA1:	d5b34d7dd4d425.
SHA256:	bcd31729e66336..
Tags:	DHL exe Formbook
Infos:	



Detection



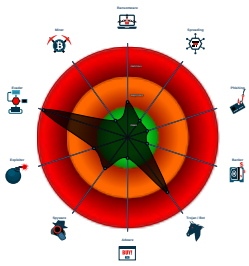
FormBook

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Self deletion via cmd or bat file
- Tries to detect sandboxes and other…
- Modifies the prolog of user mode fun…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- DHL WB# 2343640950.exe (PID: 7048 cmdline: "C:\Users\user\Desktop\DHL WB# 2343640950.exe" MD5: 81E4012E3036BEFD629438ACE2E798E2)
  - DHL WB# 2343640950.exe (PID: 6376 cmdline: C:\Users\user\Desktop\DHL WB# 2343640950.exe MD5: 81E4012E3036BEFD629438ACE2E798E2)
  - DHL WB# 2343640950.exe (PID: 6380 cmdline: C:\Users\user\Desktop\DHL WB# 2343640950.exe MD5: 81E4012E3036BEFD629438ACE2E798E2)
    - explorer.exe (PID: 3688 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmstp.exe (PID: 7120 cmdline: C:\Windows\SysWOW64\cmstp.exe MD5: 4833E65ED211C7F118D4A11E6FB58A09)
        - cmd.exe (PID: 4124 cmdline: /c del "C:\Users\user\Desktop\DHL WB# 2343640950.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 3844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.studiomayuko.com/183b/"
  ],
  "decoy": [
    "textilestyle.online",
    "decorarteperu.com",
    "commonsensedigitalmarketing.biz",
    "yumkb.com",
    "brambletonsummercamp.com",
    "fug.life",
    "grandforest.space",
    "opmbettersvault.com",
    "rheintv.com",
    "blagodatbilja.store",
    "maxpw.com",
    "vital-roots.com",
    "lotte-finance5.com",
    "socalcrypto.network",
    "extra-pays.site",
    "mmaster.xyz",
    "electriccarsinfohubs.com",
    "qshid.life",
    "digitalqp.com",
    "golfsaudiarabia.com",
    "dreaminfolks.com",
    "smartlearningtoy.com",
    "paycheckstubonlin.com",
    "allsagesbookstore.com",
    "evicts.xyz",
    "universalorlandoyout.com",
    "mannaka-chokusou.com",
    "zhisou100.xyz",
    "century21judgefit.com",
    "taphrconsultancy.com",
    "simettrixstudio.com",
    "thebestutensilios.com",
    "diabeticinsurancebroker.com",
    "importantmarks.com",
    "masterpier.com",
    "spd201.com",
    "annuelcridetreport.com",
    "c2cvision.com",
    "smithridge.net",
    "teamsfos.com",
    "asiritatli.com",
    "dreamcastlesproperties.com",
    "care-supporters.com",
    "vw-4s.com",
    "216627.com",
    "xnotconotyogurt.com",
    "veganfund.net",
    "bricksofathens.com",
    "avroty.online",
    "thinkerquote.com",
    "registerbosc.com",
    "atlantarunningtours.com",
    "citragaming.com",
    "orientadorluismi.com",
    "eternaprimaverapr.com",
    "mysuperplate.com",
    "xydict.net",
    "clairetrost.com",
    "khopkhangtho.space",
    "budhu-law.com",
    "gaozhong.online",
    "sammserviices.com",
    "whiseltiess.com",
    "businessmindfulness.store"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.508076221.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.508076221.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.508076221.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000002.508816712.000000000012F0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000002.508816712.000000000012F0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.DHL WB# 2343640950.exe.6fd0000.9.raw.unpack	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x51aaf:$s1: file:/// • 0x519bf:$s2: {11111-22222-10009-11112} • 0x51a3f:$s3: {11111-22222-50001-00000} • 0x4ee11:$s4: get_Module • 0x4f257:$s5: Reverse • 0x512ee:$s6: BlockCopy • 0x51132:$s7: ReadByte • 0x51ac1:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...
5.0.DHL WB# 2343640950.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.0.DHL WB# 2343640950.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00

Source	Rule	Description	Author	Strings
5.0.DHL WB# 2343640950.exe.400000.4.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
5.0.DHL WB# 2343640950.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 26 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

Self deletion via cmd or bat file

Modifies the prolog of user mode functions (user mode inline hooks)

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

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

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

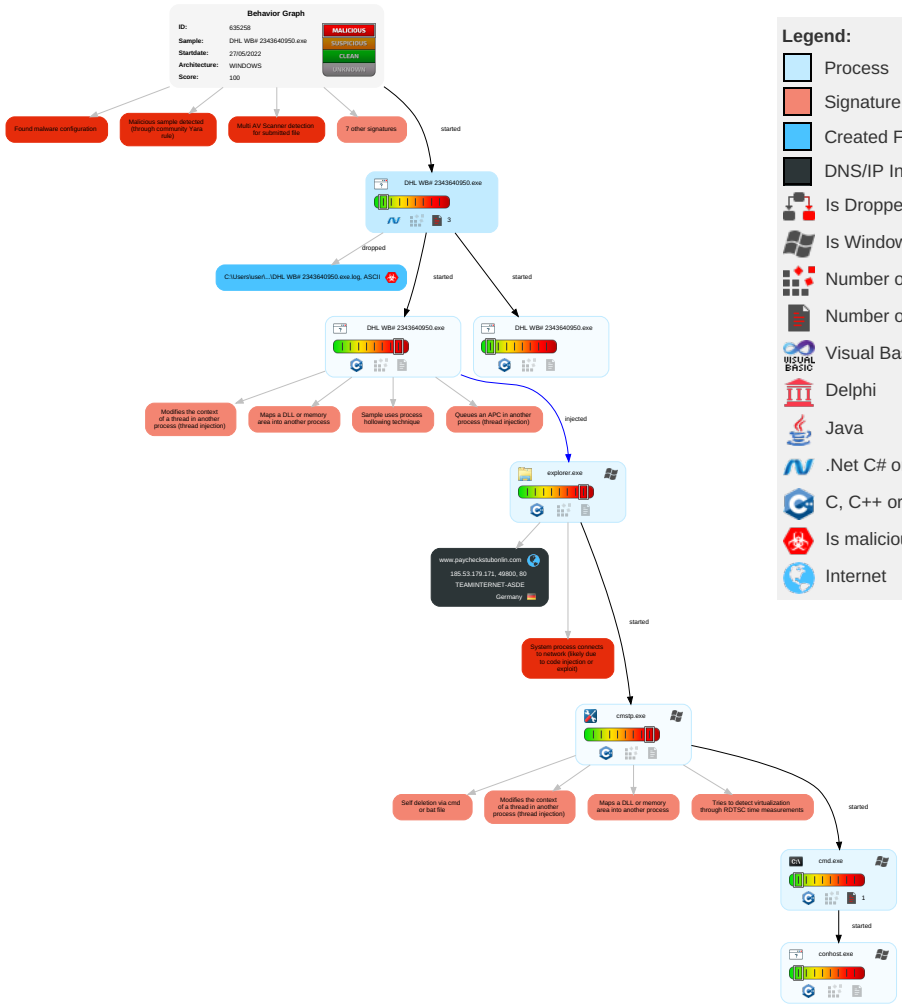
Yara detected FormBook

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 Rootkit	1 Credential API Hooking	1 Query Registry	Remote Services	1 Credential API Hooking	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 Masquerading	1 Input Capture	2 2 1 Security Software Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	1 Archive Collected Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 1 Virtualization/Sandbox Evasion	NTDS	3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	5 1 2 Process Injection	LSA Secrets	1 Remote System 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	1 Deobfuscate/Decode 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	4 Obfuscated Files or Information	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 3 Software Packing	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

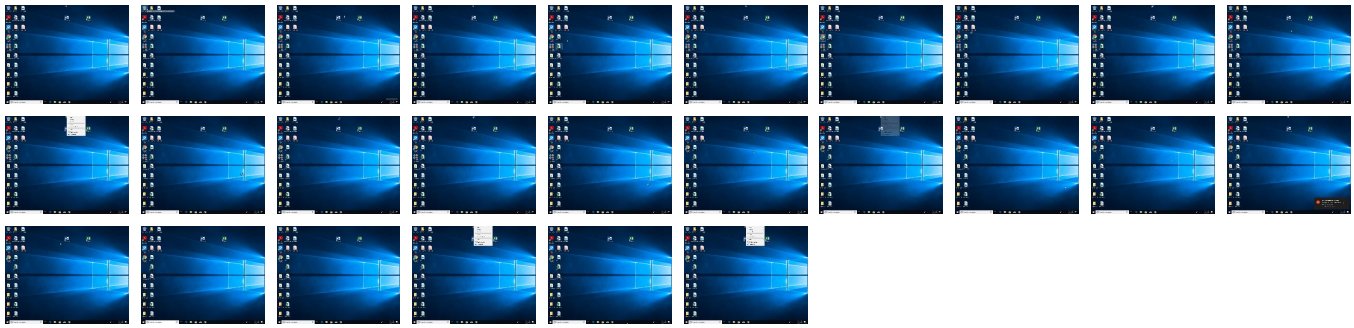
Behavior Graph



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 WB# 2343640950.exe	48%	Virustotal		Browse
DHL WB# 2343640950.exe	22%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.DHL WB# 2343640950.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.DHL WB# 2343640950.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.0.DHL WB# 2343640950.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
5.2.DHL WB# 2343640950.exe.1383ee0.2.unpack	100%	Avira	HEUR/AGEN.1234539		Download File

Source	Detection	Scanner	Label	Link	Download
5.2.DHL WB# 2343640950.exe.3740000.5.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
13.0.cmstp.exe.1250000.0.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
13.2.cmstp.exe.1250000.0.unpack	100%	Avira	HEUR/AGEN.1234539		Download File
5.2.DHL WB# 2343640950.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com4	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comw	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.carterandcone.comttp	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.paycheckstubonlin.com/183b/?3f=0pQLi>WHLhf=aeRI+VtYzSQE3A1d41SuiJFmY5rxFnxGMgk+ebPO7waK3tnPCQEIkRgDBSC82MoPtV6fY2DLrg==	0%	Avira URL Cloud	safe	
www.studiomayuko.com/183b/	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sajatypeworks.comhy/	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fonts.comT?	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.com&	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fonts.com8	0%	URL Reputation	safe	
http://www.founder.com.cn/cn%	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.paycheckstubonlin.com	185.53.179.171	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.paycheckstubonlin.com/183b/?3f=0pQLi>WHLhf=aeRI+VtYzSQE3A1d41SuiJFmY5rxFnxGMgk+ebPO7waK3tnPCQEIkRgDBSC82MoPtV6fY2DLrg==	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
www.studiomayuko.com/183b/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

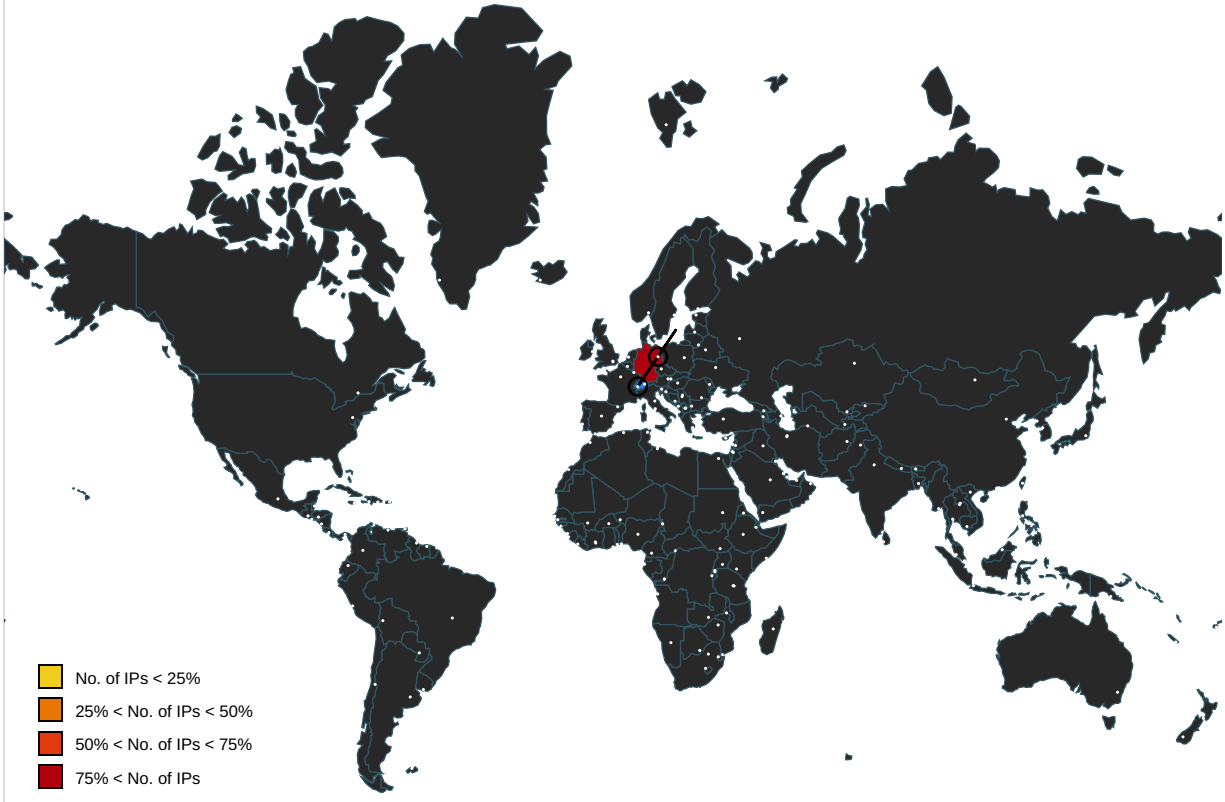
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.375029769.00000000055B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	DHL WB# 2343640950.exe, 00000000.00000003.386580488.00000000055E5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com4	DHL WB# 2343640950.exe, 00000000.00000003.371017515.00000000055DD000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.370858429.00000000055DE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comw	DHL WB# 2343640950.exe, 00000000.00000003.371017515.00000000055DD000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.370840690.00000000055DD000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.370858429.00000000055DE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.com	DHL WB# 2343640950.exe, 00000000.00000003.377133904.00000000055A7000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.377503899.00000000055A7000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.378545531.00000000055A8000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.376858559.00000000055A6000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.378033564.00000000055A6000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.377574826.00000000055A6000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.378644300.00000000055A8000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.376377568.00000000055A4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.378324382.00000000055A8000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.376750190.00000000055A4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.377095056.00000000055A7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	DHL WB# 2343640950.exe, 00000000.00000003.371017515.00000000055DD000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.370840690.00000000055DD000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.370831210.00000000055DD000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.370858429.00000000055DE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comttp	DHL WB# 2343640950.exe, 00000000.00000003.377133904.00000000055A7000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.377503899.00000000055A7000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.378545531.00000000055A8000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.380503275.00000000055A7000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.376858559.00000000055A6000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.379031205.00000000055A8000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.378033564.00000000055A6000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.377574826.00000000055A6000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.378644300.00000000055A8000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.376377568.00000000055A4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.378324382.00000000055A8000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.381687286.00000000055A6000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.376750190.00000000055A4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.377095056.00000000055A7000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrita	DHL WB# 2343640950.exe, 00000000.00000002.427545975.00000000055A0000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.420192767.00000000055A0000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	DHL WB# 2343640950.exe, 00000000.00000003.374059324.00000000055AF000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DHL WB# 2343640950.exe, 00000000.00000003.383046028.00000000055D4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.383254350.00000000055D4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.383176460.00000000055D4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.383369016.00000000055D4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.383430136.00000000055D4000.00000004.00000800.00020000.00000000.sdmp, DHL WB# 2343640950.exe, 00000000.00000003.383112465.00000000055D4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.comhy/	DHL WB# 2343640950.exe, 00000000.00000003.370858429.00000000055DE000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.comT?	DHL WB# 2343640950.exe, 00000000.00000003.371854007.00000000055DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com&	DHL WB# 2343640950.exe, 00000000.00000003.371017515.00000000055DD000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersp	DHL WB# 2343640950.exe, 00000000.00000003.382147355.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	DHL WB# 2343640950.exe, 00000000.00000002.427842888.00000000067B2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	DHL WB# 2343640950.exe, 00000000.00000003.382147355.00000000055A9000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com8	DHL WB# 2343640950.exe, 00000000.00000003.371964876.00000000055DD000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn%	DHL WB# 2343640950.exe, 00000000.00000003.374059324.00000000055AF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.53.179.171	www.paycheckstubonlin.com	Germany		61969	TEAMINTERNET-ASDE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635258
Start date and time: 27/05/202217:56:26	2022-05-27 17:56:26 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 18s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL WB# 2343640950.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:	22
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@9/1@1/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 23% (good quality ratio 20.2%) • Quality average: 68.3% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, ris.api.iris.microsoft.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target DHL WB# 2343640950.exe, PID 6376 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:57:49	API Interceptor	2x Sleep call for process: DHL WB# 2343640950.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 WB# 2343640950.exe.log

Process:	C:\Users\user\Desktop\DHL WB# 2343640950.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2148
Entropy (8bit):	5.349175784572625
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjAHKx1qHitHoxHhAHKzvFHxvAHj:iqXeqm00YqhQnouRqjAqxwCtlxHeqzNI
MD5:	945DECF362D4312BCF2BC59AAB588224
SHA1:	B8A9CD1EC92D5778D394F7F564CA4EB5D83BAE6A
SHA-256:	D85162B3E02C7B540C88441C74C2B7AD0270D70CA94A960BE08C31B2BA53DFE6
SHA-512:	300B7409CC405BDE24C2FAA3419E4C5CD0F35CAE57EBB66EE76E1CC731F1C48E395FB6CA5937E29F354D99EDCA27FE16CD4D2C59AE65598391695ECCD23B47B8
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.853412902188726
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 WB# 2343640950.exe
File size:	708608
MD5:	81e4012e3036befd629438ace2e798e2
SHA1:	d5b34d7dd4d4255fd3279bdd99c98b9e760bb34c
SHA256:	bcd31729e663369b99fd178377977c5de078512046d2cb4b38c51d80d9801374
SHA512:	7177aefff308114d491876111933db7a30acf312b9d330b01e2ffcc3915aac1af5794cee04e7c1abc8c1088998df560a5afa7de57bc03242eaf376a2f7d236f2

SSDEEP:	12288:jML1Aw768uPZbHoViBdtz4X6RfBnlw/lqOqUC03Ojrx/4c/6bTmA:jML17MZbHoVivtzhf5lw/lq1XoK3/6v/
TLSH:	49E4122D22EC0628FBFE5B7E10B95500077AAB4B6117D70F5EC574D82C83B524E16BAB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....0.....D..... .....@.. .....@.....@.....

File Icon

Icon Hash:	ccaacecccca8aecc

Static PE Info

General

Entrypoint:	0x4aa8de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x628F0D1D [Thu May 26 05:16:13 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
or al, byte ptr [eax]
add byte ptr [eax], al
adc al, 00h
add byte ptr [eax], al
push ds
add byte ptr [eax], al
add byte ptr [eax], ch
add byte ptr [eax], al
add byte ptr [eax+eax], bh
add byte ptr [eax], al
push eax
add byte ptr [eax], al
add al, ch
add eax, dword ptr [eax]
add al, ch
add eax, dword ptr [eax]
add byte ptr [eax+00h], dl
add byte ptr [eax], al
cmp al, 00h
add byte ptr [eax], al
sub byte ptr [eax], al
add byte ptr [eax], al
push ds

Instruction
add byte ptr [eax], al
add byte ptr [eax+eax], dl
add byte ptr [eax], al
or al, byte ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add eax, dword ptr [eax]
add byte ptr [eax], al
add eax, 07000000h
add byte ptr [eax], al
add byte ptr [eax], cl
add byte ptr [eax], al
add byte ptr [edx], cl
add byte ptr [eax], al
add byte ptr [eax+eax], cl
add byte ptr [eax], al
push cs
add byte ptr [eax], al
add byte ptr [ecx], dl
add byte ptr [eax], al
add byte ptr [ebx], dl
add byte ptr [eax], al
add byte ptr [17000000h], dl
add byte ptr [eax], al
add byte ptr [eax], bl
add byte ptr [eax], al
add byte ptr [edx], bl
add byte ptr [eax], al
add byte ptr [eax+eax], bl
add byte ptr [eax], al
push ds
add byte ptr [eax], al
add byte ptr [ecx], ah
add byte ptr [eax], al
add byte ptr [ebx], ah
add byte ptr [eax], al
add byte ptr [27000000h], ah
add byte ptr [eax], al
add byte ptr [eax], ch
add byte ptr [eax], al
add byte ptr [edx], ch
add byte ptr [eax], al
add byte ptr [eax+eax], ch
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], dh
add byte ptr [eax], al
add byte ptr [ebx], dh
add byte ptr [eax], al
add byte ptr [37000000h], dh
add byte ptr [eax], al
add byte ptr [eax], bh
add byte ptr [eax], al
add byte ptr [edx], bh
add byte ptr [eax], al
add byte ptr [eax+eax], bh

Instruction
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	0xaa88c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x4110	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb2000	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	0xa89a4	0xa8a00	False	0.894545728317	data	7.85849718872	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x4110	0x4200	False	0.947620738636	data	7.78997497493	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xac0c8	0x3cb9	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xafd94	0x14	data		
RT_VERSION	0xafdb8	0x354	data		

Imports

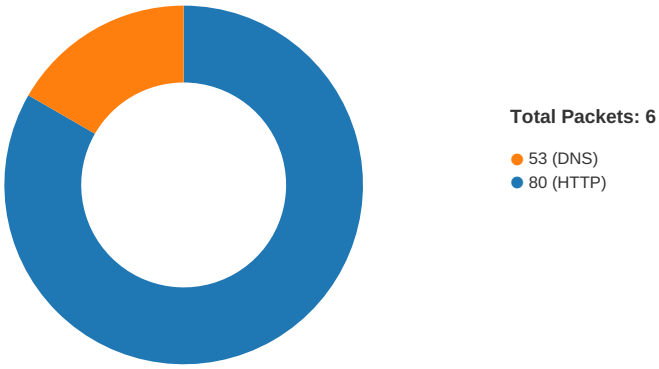
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Karel Pospil 2011
Assembly Version	1.1.0.0
InternalName	FixupD.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	Gothic
Comments	
ProductName	Gothic Checkers
ProductVersion	1.0.0.0
FileDescription	Gothic Checkers
OriginalFilename	FixupD.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:59:34.806126118 CEST	49800	80	192.168.2.6	185.53.179.171
May 27, 2022 17:59:34.822361946 CEST	80	49800	185.53.179.171	192.168.2.6
May 27, 2022 17:59:34.822493076 CEST	49800	80	192.168.2.6	185.53.179.171
May 27, 2022 17:59:34.839256048 CEST	80	49800	185.53.179.171	192.168.2.6
May 27, 2022 17:59:34.839370966 CEST	49800	80	192.168.2.6	185.53.179.171
May 27, 2022 17:59:34.856012106 CEST	80	49800	185.53.179.171	192.168.2.6
May 27, 2022 17:59:34.856033087 CEST	80	49800	185.53.179.171	192.168.2.6
May 27, 2022 17:59:34.856046915 CEST	80	49800	185.53.179.171	192.168.2.6
May 27, 2022 17:59:34.856256008 CEST	49800	80	192.168.2.6	185.53.179.171
May 27, 2022 17:59:34.856282949 CEST	49800	80	192.168.2.6	185.53.179.171
May 27, 2022 17:59:34.872529984 CEST	80	49800	185.53.179.171	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 17:59:34.761593103 CEST	52698	53	192.168.2.6	8.8.8.8
May 27, 2022 17:59:34.789715052 CEST	53	52698	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 17:59:34.761593103 CEST	192.168.2.6	8.8.8.8	0x1c6a	Standard query (0)	www.paycheckstubonlin.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 17:59:34.789715052 CEST	8.8.8.8	192.168.2.6	0x1c6a	No error (0)	www.paycheckstubonlin.com		185.53.179.171	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.paycheckstubonlin.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49800	185.53.179.171	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 27, 2022 17:59:34.839370966 CEST	7197	OUT	GET /183b/?3f=0pQLi&GTWHLhf=aeRI+VtYzSQE3A1d41SuiJFmY5rxFnxGMgk+ebPO7waK3tnPCQEIkRgDBSC82MoPtV6fY2DLrg== HTTP/1.1 Host: www.paycheckstubonlin.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 27, 2022 17:59:34.856033087 CEST	7197	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Fri, 27 May 2022 15:59:34 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

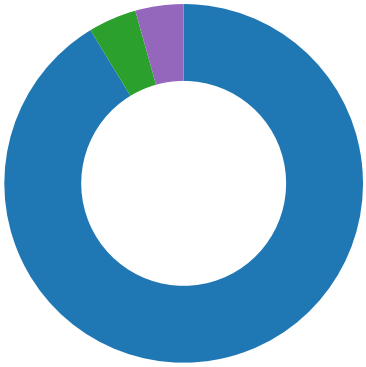
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xED
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xED
GetMessageW	INLINE	0x48 0x8B 0xB8 0x88 0x8E 0xED
GetMessageA	INLINE	0x48 0x8B 0xB8 0x80 0x0E 0xED

Statistics

Behavior

- DHL WB# 2343640950.exe
- DHL WB# 2343640950.exe
- DHL WB# 2343640950.exe
- explorer.exe
- cmstp.exe
- cmd.exe
- conhost.exe



Click to jump to process

System Behavior

Analysis Process: DHL WB# 2343640950.exe PID: **7048**, Parent PID: **2760**

General

Target ID:	0
Start time:	17:57:36
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DHL WB# 2343640950.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL WB# 2343640950.exe"
Imagebase:	0x2b0000
File size:	708608 bytes
MD5 hash:	81E4012E3036BEFD629438ACE2E798E2
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: 00000000.00000002.425718736.0000000003980000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.425718736.0000000003980000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.425718736.0000000003980000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.423321322.0000000002797000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.425338191.0000000003855000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.425338191.0000000003855000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.425338191.0000000003855000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.428458566.0000000006FD0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
Reputation:	low

File Activities

Analysis Process: DHL WB# 2343640950.exe PID: **6376**, Parent PID: **7048**

General

Target ID:	4
Start time:	17:57:56
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DHL WB# 2343640950.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\DHL WB# 2343640950.exe
Imagebase:	0x270000
File size:	708608 bytes
MD5 hash:	81E4012E3036BEFD629438ACE2E798E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: DHL WB# 2343640950.exe PID: **6380**, Parent PID: **7048**

General

Target ID:	5
Start time:	17:57:58
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DHL WB# 2343640950.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL WB# 2343640950.exe
Imagebase:	0xd80000
File size:	708608 bytes
MD5 hash:	81E4012E3036BEFD629438ACE2E798E2
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: 00000005.00000002.508076221.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.508076221.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.508076221.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.508816712.00000000012F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.508816712.00000000012F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.508816712.00000000012F0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.417761109.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.417761109.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.417761109.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.417286385.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.417286385.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.417286385.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.508664053.00000000012C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.508664053.00000000012C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.508664053.00000000012C0000.00000040.10000000.00040000.00000000.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	41A457	NtReadFile

Analysis Process: explorer.exe PID: **3688**, Parent PID: **6380**

General	
Target ID:	8
Start time:	17:58:03
Start date:	27/05/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff77c400000
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: 00000008.00000000.493111927.000000000EBB3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.493111927.000000000EBB3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.493111927.000000000EBB3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.466672366.000000000EBB3000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.466672366.000000000EBB3000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.466672366.000000000EBB3000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: cmstp.exe PID: **7120**, Parent PID: **3688**

General	
Target ID:	13
Start time:	17:58:38
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmstp.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmstp.exe
Imagebase:	0x1250000
File size:	82944 bytes
MD5 hash:	4833E65ED211C7F118D4A11E6FB58A09
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: 0000000D.00000002.641809703.0000000000EF0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.641809703.0000000000EF0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.641809703.0000000000EF0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.640957593.0000000000610000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.640957593.0000000000610000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.640957593.0000000000610000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.641933655.0000000000F20000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.641933655.0000000000F20000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.641933655.0000000000F20000.00000004.00000800.00020000.00000000.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	62A457	NtReadFile

Analysis Process: cmd.exe PID: **4124**, Parent PID: **7120**

General

Target ID:	14
Start time:	17:58:45
Start date:	27/05/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\DHL WB# 2343640950.exe"
Imagebase:	0xed0000
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: **3844**, Parent PID: **4124**

General

Target ID:	15
Start time:	17:58:47
Start date:	27/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6406f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly