ID: 532855
Sample Name: DHL DOC 3406506482.exe
Cookbook: default.jbs
Time: 18:53:41
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

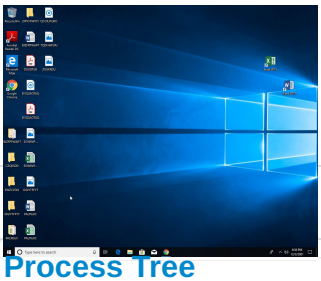
Windows Analysis Report DHL DOC 3406506482.exe

Overview

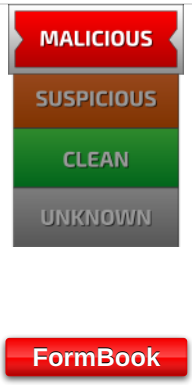
General Information

Sample Name:	DHL DOC 3406506482.exe
Analysis ID:	532855
MD5:	896c3c7f309a479..
SHA1:	9ad094b6799fb6d.
SHA256:	6f35f7c071de6ed..
Tags:	DHL exe Formbook
Infos:	

Most interesting Screenshot:



Detection



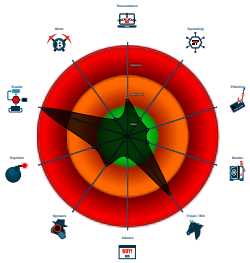
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- 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…
- Tries to detect sandboxes and other…
- Performs DNS queries to domains w…
- Modifies the prolog of user mode fun…

Classification



Process Tree

- **System is w10x64**
- DHL DOC 3406506482.exe (PID: 4824 cmdline: "C:\Users\user\Desktop\DHL DOC 3406506482.exe" MD5: 896C3C7F309A479F0AB1A9D8693B130F)
  - DHL DOC 3406506482.exe (PID: 3488 cmdline: C:\Users\user\Desktop\DHL DOC 3406506482.exe MD5: 896C3C7F309A479F0AB1A9D8693B130F)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - explorer.exe (PID: 1004 cmdline: C:\Windows\SysWOW64\explorer.exe MD5: 166AB1B9462E5C1D6D18EC5EC0B6A5F7)
        - cmd.exe (PID: 4140 cmdline: /c del "C:\Users\user\Desktop\DHL DOC 3406506482.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1688 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.verdugofarms.com/q35x/"
  ],
  "decoy": [
    "86ffd.com",
    "riquelmetaylor.com",
    "web3media.xyz",
    "lesbian-kyonyu.net",
    "assurancestreet.com",
    "giftboxpromos.com",
    "3exnck.com",
    "androidgays.com",
    "eduexsoft.com",
    "bmtmarmall.com",
    "mstrevent.com",
    "suvyco.link",
    "urautloads.com",
    "peaacockrv.com",
    "stanefree.com",
    "ybcxzgnmu.com",
    "pittsburgh-pestcontrol-co.com",
    "thesecond-handrose.com",
    "otcovotakkia.quest",
    "josephinesart.com",
    "uenpb.xyz",
    "gzczjsfg.com",
    "emptybestliving.com",
    "thecripsarena.com",
    "1688bfb.com",
    "garymullin.com",
    "socialteers-millunu.com",
    "zapf-nachhilfe.com",
    "expressportaldeliveryline.com",
    "hobbydiscover.store",
    "qncqroup.com",
    "housepainteroshawa.com",
    "craftedbycharter.com",
    "sushibaraustin.com",
    "kjjsclosets.com",
    "leylaatakan.com",
    "luminbowstore.com",
    "autoauctioncenter.com",
    "bon-da.com",
    "spilledreviews.com",
    "hbtysj.com",
    "truthrevealedtv.com",
    "gmcanchorage.com",
    "kirbycarpet.com",
    "ambire.email",
    "awonky.com",
    "giannagragnani.com",
    "infomw-abogados.com",
    "summit-mulundwest.info",
    "omradesutveckling.com",
    "jennypennybeachboutique.com",
    "medicalmarijuana.quest",
    "tusjentagal.quest",
    "zghglw.com",
    "bmcq1.com",
    "counsellinggta.com",
    "econnect.club",
    "xn--42cgr3fjyvj4c9a.com",
    "wed8029.com",
    "jeweleryshowcase.com",
    "ketofam.com",
    "roiward.tech",
    "artemi.club",
    "maddocksmedia.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.513609784.0000000002D70000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.513609784.0000000002D70000.00000040.00020000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000E.00000002.513609784.0000000002D70000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$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:$sqlite3blob: 68 53 D8 7F 8C
00000001.00000000.245861481.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000000.245861481.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.DHL DOC 3406506482.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.2.DHL DOC 3406506482.exe.400000.0.raw.unpack	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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
1.2.DHL DOC 3406506482.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$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:$sqlite3blob: 68 53 D8 7F 8C
1.0.DHL DOC 3406506482.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
1.0.DHL DOC 3406506482.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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 17 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

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

Performs DNS queries to domains with low reputation

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:

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

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:

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

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

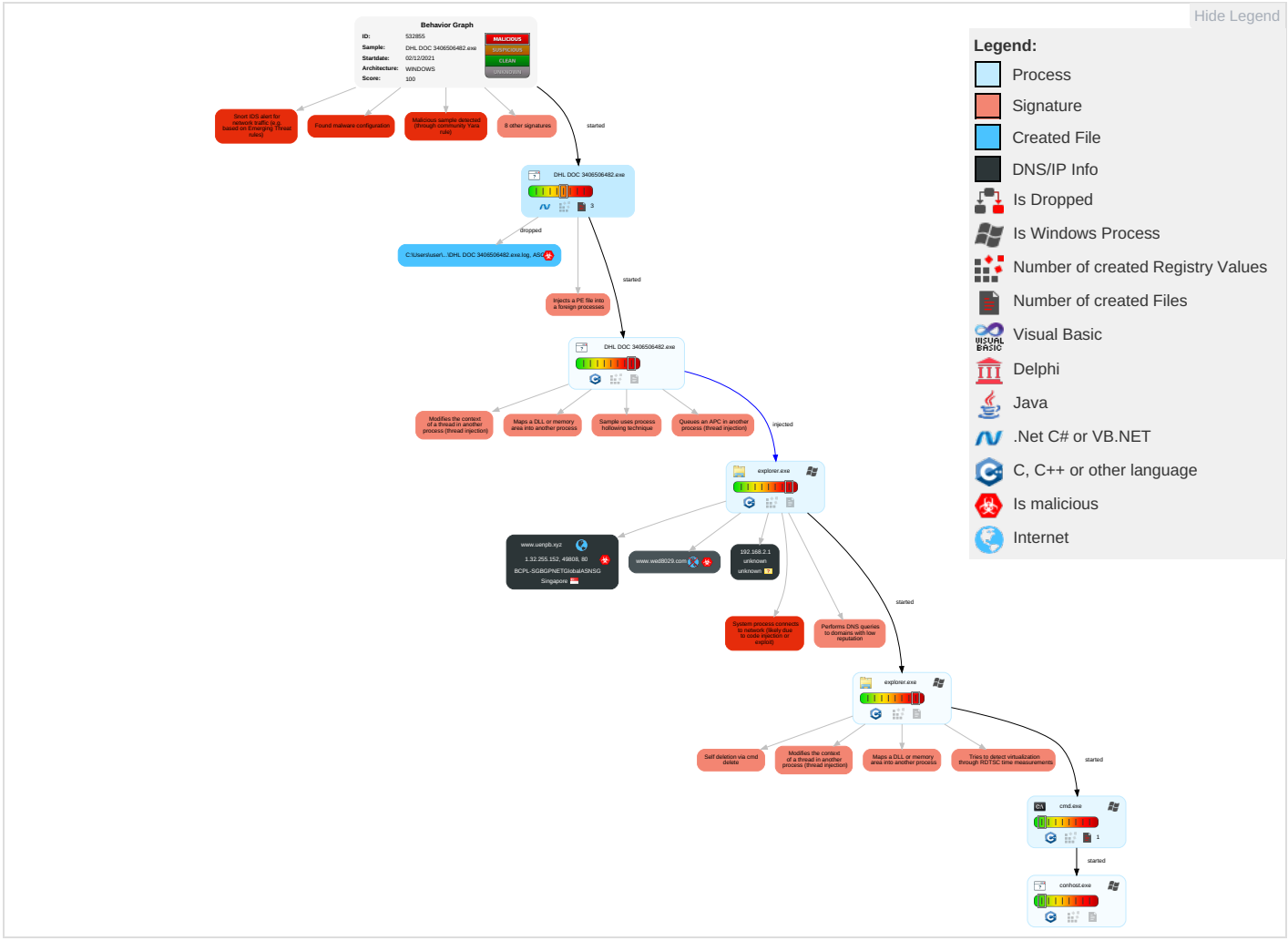
Remote Access Functionality:

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
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 4	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

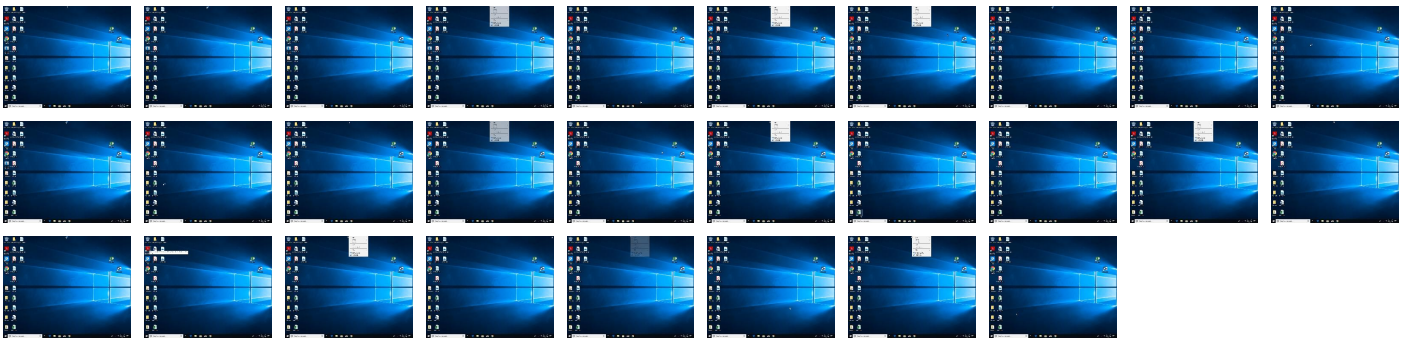
Behavior Graph



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 DOC 3406506482.exe	29%	Virustotal		Browse
DHL DOC 3406506482.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.Lazy	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.2.explorer.exe.290000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.0.explorer.exe.290000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.DHL DOC 3406506482.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.DHL DOC 3406506482.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.DHL DOC 3406506482.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.DHL DOC 3406506482.exe.33e0000.4.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.DHL DOC 3406506482.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
www.wed8029.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.uenpb.xyz/q35x/?1bL4BX=n0W6sBJt6o5hFrgQrmHErIHHCJqVSMT16xl2hKdZI7rsj0AVnZwRK3Rm3lIsVsqUahNr&TBZ8=3fcPMN	0%	Avira URL Cloud	safe	
www.verdugofarms.com/q35x/	3%	Virustotal		Browse
www.verdugofarms.com/q35x/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.uenpb.xyz	1.32.255.152	true	true		unknown
www.wed8029.com	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.uenpb.xyz/q35x/?1bL4BX=n0W6sBJt6o5hFrgQrmHErIHHCJqVSMT16xl2hKdZI7rsj0AVnZwRK3Rm3lIsVsqUahNr&TBZ8=3fcPMN	true	• Avira URL Cloud: safe	unknown
www.verdugofarms.com/q35x/	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	low

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
1.32.255.152	www.uenpb.xyz	Singapore		64050	BCPL-SGBGPNETGlobalASNSG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532855
Start date:	02.12.2021
Start time:	18:53:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL DOC 3406506482.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:	26
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@7/1@5/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 65.9% (good quality ratio 61.3%) • Quality average: 71.6% • Quality standard deviation: 30.8%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:54:37	API Interceptor	1x Sleep call for process: DHL DOC 3406506482.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
BCPL-SGBGPNETGlobalASNSG	t6rrqsi3Bp	Get hash	malicious	Browse	• 134.122.132.42
	REQ. FOR QUOTATION.exe	Get hash	malicious	Browse	• 1.32.254.254
	Ljm7n1QDZe	Get hash	malicious	Browse	• 134.122.144.26
	dd#U5149.exe	Get hash	malicious	Browse	• 118.107.44.235
	c6#U9891.exe	Get hash	malicious	Browse	• 118.107.44.235
	f4#U6b7b.exe	Get hash	malicious	Browse	• 118.107.44.235
	gOJtZzW63F.exe	Get hash	malicious	Browse	• 202.79.175.12
	c85WWDlKf2.dll	Get hash	malicious	Browse	• 202.36.49.75
	SecuriteInfo.com.Trojan.GenericKDZ.80412.21668.dll	Get hash	malicious	Browse	• 202.36.49.75
	swift copy.exe	Get hash	malicious	Browse	• 1.32.254.254
	TFEkbH3ag3	Get hash	malicious	Browse	• 69.176.83.27
	00#U4e0b.exe	Get hash	malicious	Browse	• 118.107.44.235
	c6#U9891.exe	Get hash	malicious	Browse	• 202.79.171.220
	#U56fd#U5916#U66b4#U5229#U884c#U4e1a#U5962#U9761#U751f#U6d3b#U8bb0#U5f55#U89c6#U9891.exe	Get hash	malicious	Browse	• 202.79.165.153
	e6#U60c5.exe	Get hash	malicious	Browse	• 202.79.171.220
	5b#U6655.exe	Get hash	malicious	Browse	• 69.176.89.208
	52#U7eff.exe	Get hash	malicious	Browse	• 118.107.44.235

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Payment Order.exe	Get hash	malicious	Browse	• 134.122.133.133
	kA1GNOTJ2VgnL02.exe	Get hash	malicious	Browse	• 1.32.254.254
	GB0O1NUtmJ	Get hash	malicious	Browse	• 137.220.211.75

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL DOC 3406506482.exe.log	
Process:	C:\Users\user\Desktop\DHL DOC 3406506482.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
Malicious:	**true**
Reputation:	moderate, 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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.840952482967267
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% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHL DOC 3406506482.exe
File size:	692736
MD5:	896c3c7f309a479f0ab1a9d8693b130f
SHA1:	9ad094b6799fb6deea1d2c3704576db3353d70ae
SHA256:	6f35f7c071de6ed456c189e023daa27c5b0cd007d4fcddbb13316a82ada83abe
SHA512:	c094e97eb898870a466dbc0f981ec379298805e4f5a0c5fc55291575d19dc94face2615f9db04b602ab489bd7e8d66248fa4acea3cb44117dd2106c9d08cba1c
SSDEEP:	12288:h4dN+434/7u9SOQ1saJoOqqMY0hwCvO3m36HNYi+Kebigu80DfDhJXX:hU44W7oioLq+hhWm36E3bo8WfDb

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Q(.a.....0..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4aa582
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:	0x61A82851 [Thu Dec 2 01:58:41 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa8588	0xa8600	False	0.915302234131	data	7.85043153763	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x618	0x800	False	0.3408203125	data	3.46786443123	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-18:56:18.995145	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
12/02/21-18:56:20.025625	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-18:56:22.026347	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.5	8.8.8.8
12/02/21-18:56:34.770599	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.5	1.32.255.152
12/02/21-18:56:34.770599	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.5	1.32.255.152
12/02/21-18:56:34.770599	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.5	1.32.255.152

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 18:56:12.963686943 CET	192.168.2.5	8.8.8.8	0x60c6	Standard query (0)	www.wed8029.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:56:13.975543022 CET	192.168.2.5	8.8.8.8	0x60c6	Standard query (0)	www.wed8029.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:56:15.006789923 CET	192.168.2.5	8.8.8.8	0x60c6	Standard query (0)	www.wed8029.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:56:17.007019997 CET	192.168.2.5	8.8.8.8	0x60c6	Standard query (0)	www.wed8029.com	A (IP address)	IN (0x0001)
Dec 2, 2021 18:56:34.172086954 CET	192.168.2.5	8.8.8.8	0x1ecf	Standard query (0)	www.uenpb.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:56:17.983330965 CET	8.8.8.8	192.168.2.5	0x60c6	Server failure (2)	www.wed8029.com	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 18:56:18.995060921 CET	8.8.8.8	192.168.2.5	0x60c6	Server failure (2)	www.wed8029.com	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 18:56:20.025499105 CET	8.8.8.8	192.168.2.5	0x60c6	Server failure (2)	www.wed8029.com	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 18:56:22.026230097 CET	8.8.8.8	192.168.2.5	0x60c6	Server failure (2)	www.wed8029.com	none	none	A (IP address)	IN (0x0001)
Dec 2, 2021 18:56:34.510354042 CET	8.8.8.8	192.168.2.5	0x1ecf	No error (0)	www.uenpb.xyz		1.32.255.152	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49808	1.32.255.152	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:56:34.770598888 CET	16140	OUT	GET /q35x/?1bL4BX=n0W6sBJt6o5hFrgQrmHErIHHCJqVSMT16xl2hKdZI7rsj0AVnZwRK3Rm3lIsVsqUahNr&TBZ8=3fcPMN HTTP/1.1 Host: www.uenpb.xyz Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 18:56:35.024651051 CET	16140	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 02 Dec 2021 17:56:34 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 34 20 4e 6f 74 20 46 6f 75 6e 64 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 34 20 4e 6f 74 20 46 6f 75 6e 64 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>404 Not Found</title></head><body> 404 Not Found <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

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DHL DOC 3406506482.exe PID: 4824 Parent PID: 6024

General

Start time:	18:54:36
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\DHL DOC 3406506482.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL DOC 3406506482.exe"
Imagebase:	0x3b0000
File size:	692736 bytes
MD5 hash:	896C3C7F309A479F0AB1A9D8693B130F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.248588915.0000000002791000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.248628674.00000000027CD000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.249416535.0000000003799000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.249416535.0000000003799000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.249416535.0000000003799000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: DHL DOC 3406506482.exe PID: 3488 Parent PID: 4824

General

Start time:	18:54:38
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\DHL DOC 3406506482.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL DOC 3406506482.exe
Imagebase:	0x490000
File size:	692736 bytes
MD5 hash:	896C3C7F309A479F0AB1A9D8693B130F
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: 00000001.00000000.245861481.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.245861481.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.245861481.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.316002438.0000000000AD0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.316002438.0000000000AD0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.316002438.0000000000AD0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.315948001.00000000009C0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.315948001.00000000009C0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.315948001.00000000009C0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.246580702.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.246580702.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.246580702.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.315617862.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.315617862.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.315617862.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 3488

General

Start time:	18:54:42
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
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: 00000002.00000000.290164309.00000000070EF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.290164309.00000000070EF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.290164309.00000000070EF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.275035294.00000000070EF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.275035294.00000000070EF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.275035294.00000000070EF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: explorer.exe PID: 1004 Parent PID: 3472

General

Start time:	18:55:08
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\explorer.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\explorer.exe
Imagebase:	0x290000
File size:	3611360 bytes
MD5 hash:	166AB1B9462E5C1D6D18EC5EC0B6A5F7
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: 0000000E.00000002.513609784.0000000002D70000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.513609784.0000000002D70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.513609784.0000000002D70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.513416867.0000000002C70000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.513416867.0000000002C70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.513416867.0000000002C70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000E.00000002.512624428.0000000000790000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000E.00000002.512624428.0000000000790000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000E.00000002.512624428.0000000000790000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4140 Parent PID: 1004

General

Start time:	18:55:14
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\DHL DOC 3406506482.exe"
Imagebase:	0x150000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 1688 Parent PID: 4140

General

Start time:	18:55:16
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis