ID: 532858
Sample Name: invoice dhl.delivery document and original invoice sign.exe
Cookbook: default.jbs
Time: 18:56:21
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Windows Analysis Report invoice dhl.delivery documen…

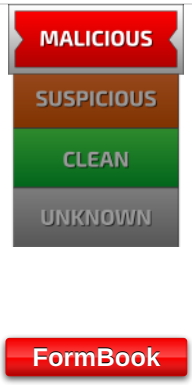
Overview

General Information

Sample Name:	invoice dhl.delivery document and original invoice sign.exe
Analysis ID:	532858
MD5:	ebce26da75669d..
SHA1:	bcc8f769e51cd9f…
SHA256:	5fef546d71e9ed9..
Tags:	DHL exe Formbook
Infos:	

Most interesting Screenshot:

Detection

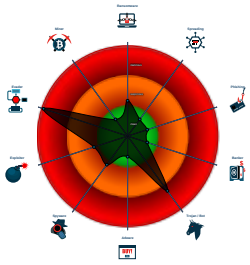


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete

Classification



- **System is w10x64**
- invoice dhl.delivery document and original invoice sign.exe (PID: 3452 cmdline: "C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.exe" MD5: EBCE26DA75669D94DBC0550BF394B204)
  - invoice dhl.delivery document and original invoice sign.exe (PID: 6188 cmdline: C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.exe MD5: EBCE26DA75669D94DBC0550BF394B204)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 7056 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 7092 cmdline: /c del "C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7108 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.cuteprofessionalscrubs.com/9gr5/"
  ],
  "decoy": [
    "newleafcosmetix.com",
    "richermanscastle.com",
    "ru-remonton.com",
    "2diandongche.com",
    "federaldados.design",
    "jeffreycookweb.com",
    "facecs.online",
    "xmeclarn.xyz",
    "olgasmith.xyz",
    "sneakersonlinesale.com",
    "playboyshiba.com",
    "angelamiglioli.com",
    "diitaldefynd.com",
    "whenevergames.com",
    "mtheartcustom.com",
    "vitalactivesupply.com",
    "twistblogr.com",
    "xn--i8s140at3d6u7c.tel",
    "baudelaireelhakim.com",
    "real-estate-miami-searcher.site",
    "131122.xyz",
    "meta-medial.com",
    "carvanaworkers.com",
    "mimamincloor.com",
    "aglutinarteshop.com",
    "portal-arch.com",
    "mandeide.com",
    "golfteesy.com",
    "carteretcancer.center",
    "cuansamping.com",
    "jhhnet.com",
    "oetthalr.xyz",
    "toesonly.com",
    "ctbizmag.com",
    "searchonzippy.com",
    "plantedapts.com",
    "matoneg.online",
    "takened.xyz",
    "meta4.life",
    "africanizedfund.com",
    "jukeboxjason.com",
    "folez.online",
    "troddu.com",
    "802135.com",
    "guiamat.net",
    "gladiasol.com",
    "meditationandyogacentre.com",
    "metaverserealestateagent.com",
    "boogyverse.net",
    "melissa-mochafest.com",
    "cozsweeps.com",
    "pickles-child.com",
    "metaversemediaschool.com",
    "ahfyfz.com",
    "ses-coating.com",
    "pozada.biz",
    "loldollmagic.com",
    "mountfrenchlodge.net",
    "25680125.xyz",
    "inusuklearning.com",
    "dnteagcud.xyz",
    "yupan.site",
    "acloud123.xyz",
    "asadosdonchorizo.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.622111638.0000000002CE0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.622111638.0000000002CE0000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000B.00000002.622111638.0000000002CE0000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$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:$sqlite3blob: 68 53 D8 7F 8C
00000005.00000000.393113317.000000000EE6F000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000005.00000000.393113317.000000000EE6F000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x21a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x292f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x141c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x992a:$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
3.0.invoice dhl.delivery document and original invoice sign.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.invoice dhl.delivery document and original invoice sign.exe.400000.8.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.invoice dhl.delivery document and original invoice sign.exe.400000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$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:$sqlite3blob: 68 53 D8 7F 8C
3.0.invoice dhl.delivery document and original invoice sign.exe.400000.4.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.invoice dhl.delivery document and original invoice sign.exe.400000.4.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$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
Click to see the 16 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

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:

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)

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

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

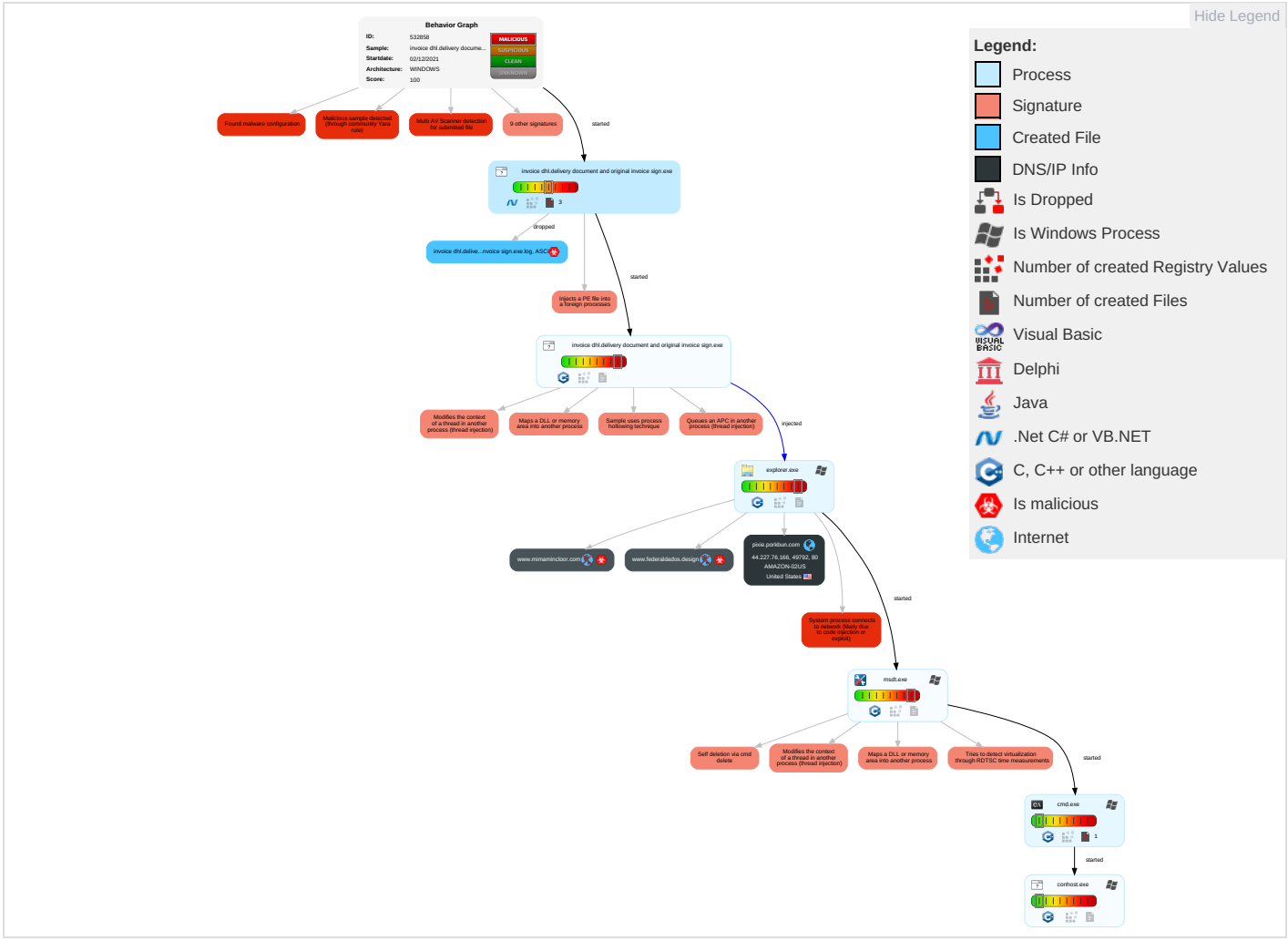
Remote Access Functionality:

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 1	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 2	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 2	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

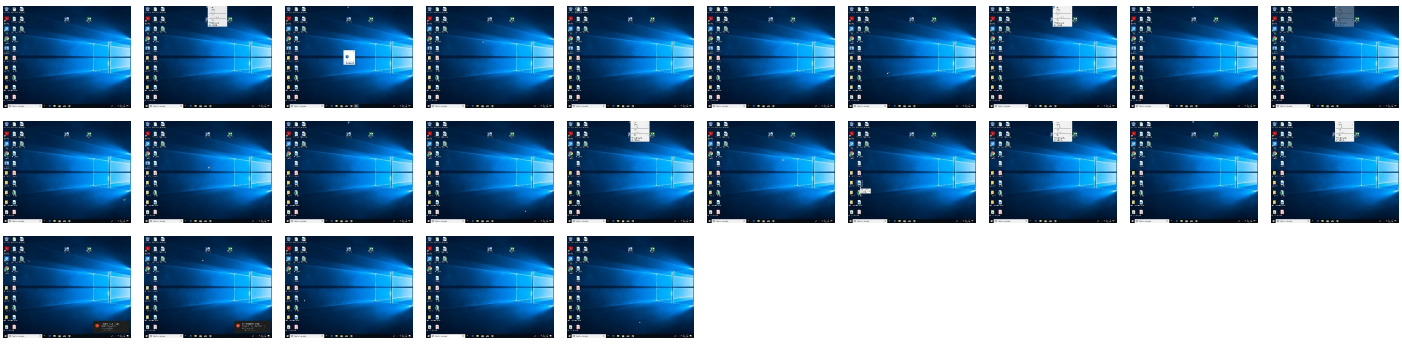
Behavior Graph



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
invoice dhl.delivery document and original invoice sign.exe	29%	ReversingLabs	Win32.Trojan.Generic	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.invoice dhl.delivery document and original invoice sign.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.invoice dhl.delivery document and original invoice sign.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.invoice dhl.delivery document and original invoice sign.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.invoice dhl.delivery document and original invoice sign.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.cuteprofessionalscrubs.com/9gr5/	0%	Avira URL Cloud	safe	
http://www.federaldados.design/9gr5/?KrIxB=GtutZXLXlTaHD4Kp&WDH=t25TG+ulm10lwD+thJsAbOsGVXQVz47UhtdUUfJn66HyA3cvvtnG3RYsUIYwzVeadKzVomQtsQ==	0%	Avira URL Cloud	safe	
http://federaldados.design	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pixie.porkbun.com	44.227.76.166	true	false		high
www.mimamincloor.com	unknown	unknown	true		unknown
www.federaldados.design	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.cuteprofessionalscrubs.com/9gr5/	true	• Avira URL Cloud: safe	low
http://www.federaldados.design/9gr5/?KrIxB=GtutZXLXlTaHD4Kp&WDH=t25TG+ulm10lwD+thJsAbOsGVXQVz47UhtdUUfJn66HyA3cvvtnG3RYsUIYwzVeadKzVomQtsQ==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
44.227.76.166	pixie.porkbun.com	United States		16509	AMAZON-02US	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532858
Start date:	02.12.2021
Start time:	18:56:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	invoice dhl.delivery document and original invoice sign.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:	24
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@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 10.1% (good quality ratio 9%) • Quality average: 69.7% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 97% • 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
18:57:23	API Interceptor	1x Sleep call for process: invoice dhl.delivery document and original invoice sign.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
44.227.76.166	draft_inv dec21.exe	Get hash	malicious	Browse	• www.apps365.one/n8ds/?gHl=UGKaYhNfstwp7hLG7UrFh27uWUnvgBcRCHkNbEmp8q6nPSt6bmPZIRKUPgjia3mN02Vr&3fkxqn=hXcDbfFHWB34bR8p
	GV20.xlsx	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?g2=3MX+rG6qdMdpgj3vkcjGUKQb8RZ/Wti45jKeFUgZ8Sp9kre80Lf7BBErzfoB75v9CaDIsg==&cL30r=9rotn4JHoV3ltP8
	DHL Documents.exe	Get hash	malicious	Browse	• www.dazzlehide.com/how6/?l2Jl=zrWVDLIDcIqBKRYG1UA+Wpo4WhIstAWIPVtKBtZyKgnKFq7ePhcu8NeTnhol46ILoLGp&Tf5pq=W6zlk8Rp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	InfoDoc-TGT23.xlsx	Get hash	malicious	Browse	• www.motan.one/e9gd/?kbMpZrx=1Tx/x2BtnTfqhKNFsgzrN2ChDpvRrwmThrJ1L/NufEAFSHMFfBw+pnINnQuUZ1NWw2fceQ==&1b=iHN83
	Tax payment invoice - Wed, November 10, 2021,pdf.exe	Get hash	malicious	Browse	• www.auribunk.com/e3rs/?mf=TRvZRMAw3lsKUL9CXC8eqAI5bRo13x6FqkgJspROms4gTvW8iipg2M7S/NGvrxuIEdWN&Nzut=7ni4n2oPNjQ
	Quote request.exe	Get hash	malicious	Browse	• www.dietjakarta.com/s2qi/?B4Zpg=n2MLk&TJELpfLP=qOzazkHAVvIGDra8b9OWW7CQPYry4NAftY2oZLUdYfYDTW+xNyVbwU9NOeXebbzy0cbp
	HCCuazHtYM.exe	Get hash	malicious	Browse	• www.kisah.xyz/sywu/?Wdcl=USn/s/Nyq2IB4uI+SZdH7vYZi5cG3dzFHZJ6S+kDyK7ak+Qptb1BIkroqQUbeC08Hzvk&f0=6lux
	AhsMBcI8HE.exe	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?FDK=8pHld4yh&IBZp=3MX+rG6vdLdtgz7jmcjGUKQb8RZ/Wti45jSOZX8Y4yp8kay6zbO3XF8pw5kHwI72X83/
	EyCIJOX8SE.exe	Get hash	malicious	Browse	• www.zerw2.com/q36e/?7nAP7b=Rntl1NDFA6KYRcsqazHh+Zc5uliS6OLgFgzbWqR6HwMZQd5uPPAwi9BbZn8pw0w7Jz4p&2dxhP=9rl0db
	Purchase Order_pdf.exe	Get hash	malicious	Browse	• www.sharpabode.com/m46c/?vZY8T=cbYwwDYfq0EA1/dzvh5+5q31ws3piQ0R8cWk1s43hoFTk6H0f8stk5G5Q6DD0FZfegy9&eDKpqJ=4hlLdHAHW

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Jrc9iR2XxH.exe	Get hash	malicious	Browse	• www.cerulecode.com/fpdi/?HfW=Y4i9pRfqC0VEN73682mG/jD+Vu59l4hEkdMs70p216zZ0VDsaaS5oQ0h3VnsQu+aBNhS&SF=4huTiLj0U
	Purchase Order-10,000MT.exe	Get hash	malicious	Browse	• www.brunchy.one/z4m5/?0BZ=zNPWEz3pIEHibvS4bsIXDPiznK4rKMrVGAhmY+HWnOPy3ASb809gbr8Dwg2gtflOJLni&GrTx=OBZlGh08BLVtF
	Draft shipping docs CI+PL.xlsx	Get hash	malicious	Browse	• www.innoattic.com/bs8f/?cB=g8xx_j&8p=gPvbgkUuDHvxuJMOi3Tla1oGEdPTt04jzJFwq+zy+XCPeJFywCVHj+bsawhRKX7OnQxPtw==
	INQ No.KP-30-00-PS-PI-INQ-0044.exe	Get hash	malicious	Browse	• www.keenlodge.com/z4m5/?IbWD=IxgNhcPCMNp9bV879hJPaVaLt/F9tNvz+B8dWaixPZ5v/4GUpiSAT9d+tp3lIab/iqeX&u48=-ZxdAxW
	1908790.exe	Get hash	malicious	Browse	• www.fleetizer.com/fg6s/?6lUXCh2=IckWWdKyCvbUOE8Ak+7kGAJP2dTotOIdi/VcdgZTnhZBerDYh6qAkCj/DPMztv+2yYxp&oL3Lu=a4mDHl20kLKIY
	eLL1MVwOME.exe	Get hash	malicious	Browse	• www.kisah.xyz/sywu/?BR=USn/s/Nyq2IB4uI+SZdH7vYZi5cG3dzFHZJ6S+kDyK7ak+Qptb1BIkroqQUxByE8Dxnk&bN90g=JTsp4zoP3f
	IRFdB0zpoK.exe	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?GJEXK=3MX+rG6vdLdtgz7jmcjGUKQb8RZ/Wti45jSOZX8Y4yp8kay6zbO3XF8pw6EX/prOJZe4&Zl=5jBl74npBZ

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PpyXtBdTaF.exe	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?o0GTN=cL3PcjiPVroHY&0VltihtH=3MX+rG6vdLdtgz7jmcjGUKQb8RZ/Wti45jSOZX8Y4yp8kay6zbO3XF8pw6EX/prOJZe4
	9QqkVnhDbm.exe	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?4h68ir=3MX+rG6vdLdtgz7jmcjGUKQb8RZ/Wti45jSOZX8Y4yp8kay6zbO3XF8pw6EX/prOJZe4&n2=YHstuLSPt
	bPIX6IObw2.exe	Get hash	malicious	Browse	• www.fleetton.com/fqiq/?aJExY=5juP-hz0rVndupn&W488=3MX+rG6vdLdtgz7jmcjGUKQb8RZ/Wti45jSOZX8Y4yp8kay6zbO3XF8pw6E9gZbONbW4

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
pixie.porkbun.com	EyCIJOX8SE.exe	Get hash	malicious	Browse	• 44.227.76.166
	TRJViVkvTr.exe	Get hash	malicious	Browse	• 44.227.76.166
	Production Inquiry.xlsx	Get hash	malicious	Browse	• 44.227.65.245
	NEW ORDER.doc	Get hash	malicious	Browse	• 44.227.65.245
	BIN.exe	Get hash	malicious	Browse	• 44.227.65.245
	v02dyhbaq5.exe	Get hash	malicious	Browse	• 44.227.65.245
	TT COPY_11010089.exe	Get hash	malicious	Browse	• 44.227.76.166
	I6B6iC23da.exe	Get hash	malicious	Browse	• 44.227.65.245
	08-14.exe	Get hash	malicious	Browse	• 44.227.65.245
	Swift Copy.xlsx	Get hash	malicious	Browse	• 44.227.76.166
	VESSEL BOOKING DETAILS_pdf.exe	Get hash	malicious	Browse	• 44.227.76.166
	OoBepaLH3W.exe	Get hash	malicious	Browse	• 44.227.76.166
	INVOICES.exe	Get hash	malicious	Browse	• 44.227.65.245
	Transfer Payment For Invoice 321-1005703.exe	Get hash	malicious	Browse	• 44.227.76.166
	productos.exe	Get hash	malicious	Browse	• 44.227.65.245
	QxVf0A9SFT.exe	Get hash	malicious	Browse	• 44.227.76.166
	Inv_7623980.exe	Get hash	malicious	Browse	• 44.227.76.166
	Inv_7623980.exe	Get hash	malicious	Browse	• 44.227.76.166
	Tlz3P6ra10.exe	Get hash	malicious	Browse	• 44.227.76.166
	Order210622.exe	Get hash	malicious	Browse	• 44.227.76.166

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-02US	oeOZvHnuaU	Get hash	malicious	Browse	• 54.171.230.55
	Milleniumbpc.xlsx	Get hash	malicious	Browse	• 44.231.165.140
	PQPv91RexG	Get hash	malicious	Browse	• 34.249.145.219
	WAYBILL 44 7611 9546 - Joao Carlos.exe	Get hash	malicious	Browse	• 75.2.115.196
	HBL No_PZU100035300.xlsx	Get hash	malicious	Browse	• 3.64.163.50
	ufKi6DmWMQCuEb4.exe	Get hash	malicious	Browse	• 3.108.154.143
	yVvATSvedsfMg0l.exe	Get hash	malicious	Browse	• 3.64.163.50
	'Vm Note'ar_dept On Wed, 01 Dec 2021 220320 +0100.html	Get hash	malicious	Browse	• 52.84.148.85
	EmployeeAssessment.html	Get hash	malicious	Browse	• 108.157.4.48

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	bUSzS84fr4.dll	Get hash	malicious	Browse	• 205.251.242.103
	M72Kclc67w.dll	Get hash	malicious	Browse	• 13.225.75.74
	5jsO2t1pju.dll	Get hash	malicious	Browse	• 13.225.75.74
	4bndVtKthy.dll	Get hash	malicious	Browse	• 13.225.75.74
	8frEuSow0b.exe	Get hash	malicious	Browse	• 13.58.157.220
	dDGwIMJCU9.exe	Get hash	malicious	Browse	• 3.22.15.135
	NtJEv6gABB.exe	Get hash	malicious	Browse	• 3.22.15.135
	e6o8rHLN98.exe	Get hash	malicious	Browse	• 3.22.15.135
	Poh Tiong Trading - products list.exe	Get hash	malicious	Browse	• 52.209.14.22
	dowNext.dll	Get hash	malicious	Browse	• 13.224.92.74
	'Vm Note'username On Wed, 01 Dec 2021 192129 +0100.html	Get hash	malicious	Browse	• 13.224.96.22

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\invoice dhl.delivery document and original invoice sign.exe.log	
Process:	C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.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:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D33784
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):	7.790881583355775
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:	invoice dhl.delivery document and original invoice sign.exe
File size:	449536

General

MD5:	ebce26da75669d94dbc0550bf394b204
SHA1:	bcc8f769e51cd9f8a160e58840f80a008e2b72e2
SHA256:	5fef546d71e9ed9f2e457bfd9aeb23a42a5074af37599c7fe4dcfeb8f687723c
SHA512:	0e87adccb6d3ca4ea2ee2e101a20ea81437e3f774dd3296c264c92ce763adacacbe1a8a4b9b6226c0b8403569c716fd5fcc55820ea4a0575172d396bae432ed0
SSDEEP:	12288:pY6XjcPK3hl0If0PufZptLKxO5J/jJUf7b3:LXjSKgIf8ufTtLPlqfP
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...i..a................................ ....@.. ....@............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46f0be
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A89569 [Thu Dec 2 09:44:09 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	0x6d0c4	0x6d200	False	0.883519473081	data	7.80084963355	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x70000	0x4c0	0x600	False	0.37890625	data	4.67278801338	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x72000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 18:58:54.919909000 CET	192.168.2.6	8.8.8.8	0x5c14	Standard query (0)	www.federaldados.design	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:16.066459894 CET	192.168.2.6	8.8.8.8	0xb04d	Standard query (0)	www.mimamincloor.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:58:54.948086977 CET	8.8.8.8	192.168.2.6	0x5c14	No error (0)	www.federaldados.design	pixie.porkbun.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:58:54.948086977 CET	8.8.8.8	192.168.2.6	0x5c14	No error (0)	pixie.porkbun.com		44.227.76.166	A (IP address)	IN (0x0001)
Dec 2, 2021 18:58:54.948086977 CET	8.8.8.8	192.168.2.6	0x5c14	No error (0)	pixie.porkbun.com		44.227.65.245	A (IP address)	IN (0x0001)
Dec 2, 2021 18:59:16.090806007 CET	8.8.8.8	192.168.2.6	0xb04d	Name error (3)	www.mimamincloor.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.federaldados.design

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49792	44.227.76.166	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:58:55.346857071 CET	11717	OUT	GET /9gr5/?KrIxB=GtutZXLXlTaHD4Kp&WDH=t25TG+ulm10lwD+thJsAbOsGVXQVz47UhtdUUfJn66HyA3cvvtnG3RYsUIYwzVeadKzVomQtsQ== HTTP/1.1 Host: www.federaldados.design Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 18:58:55.542661905 CET	11717	IN	HTTP/1.1 307 Temporary Redirect Server: openresty Date: Thu, 02 Dec 2021 17:58:55 GMT Content-Type: text/html; charset=utf-8 Content-Length: 168 Connection: close Location: http://federaldados.design X-Frame-Options: sameorigin Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 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 33 30 37 20 54 65 6d 70 6f 72 61 72 79 20 52 65 64 69 72 65 63 74 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 6f 70 65 6e 72 65 73 74 79 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>307 Temporary Redirect</title></head><body> 307 Temporary Redirect <hr> openresty </body></html>

Code Manipulations

User Modules

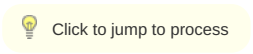
Hook Summary

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



System Behavior

Analysis Process: invoice dhl.delivery document and original invoice sign.exe PID: 3452 Parent PID: 6056

General

Start time:	18:57:22
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.exe"
Imagebase:	0x4e0000
File size:	449536 bytes
MD5 hash:	EBCE26DA75669D94DBC0550BF394B204
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: 00000000.00000002.363236510.00000000028A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.363182286.0000000002871000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.364023300.0000000003879000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.364023300.0000000003879000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.364023300.0000000003879000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: invoice dhl.delivery document and original invoice sign.exe PID: 6188 Parent PID: 3452

General

Start time:	18:57:26
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.exe
Imagebase:	0x990000
File size:	449536 bytes
MD5 hash:	EBCE26DA75669D94DBC0550BF394B204
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: 00000003.00000002.437063285.0000000001400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.437063285.0000000001400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.437063285.0000000001400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.437007987.00000000013D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.437007987.00000000013D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.437007987.00000000013D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.360478598.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.360478598.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.360478598.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.436548736.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.436548736.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.436548736.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.359940174.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.359940174.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.359940174.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities — Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6188

General

Start time:	18:57:29
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.393113317.000000000EE6F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.393113317.000000000EE6F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.393113317.000000000EE6F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.405515832.000000000EE6F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.405515832.000000000EE6F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.405515832.000000000EE6F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: msdt.exe PID: 7056 Parent PID: 3440

General

Start time:	18:58:00
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xb30000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
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: 0000000B.00000002.622111638.0000000002CE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.622111638.0000000002CE0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.622111638.0000000002CE0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.617350722.0000000000700000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.617350722.0000000000700000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.617350722.0000000000700000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.622077394.0000000002CB0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.622077394.0000000002CB0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.622077394.0000000002CB0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7092 Parent PID: 7056

General

Start time:	18:58:04
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\invoice dhl.delivery document and original invoice sign.exe"
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 7108 Parent PID: 7092

General

Start time:	18:58:06
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496

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

Disassembly

Code Analysis