ID: 635262
Sample Name: DHL - OVERDUE ACCOUNT - 130115482244.exe
Cookbook: default.jbs
Time: 18:03:41
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

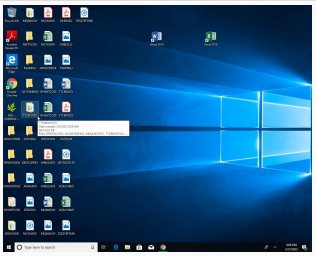
Windows Analysis Report

DHL - OVERDUE ACCOUNT - 130115482244.exe

Overview

General Information

Sample Name:	DHL - OVERDUE ACCOUNT - 130115482244.exe
Analysis ID:	635262
MD5:	3aadebe9b94245.
SHA1:	794dc763ca6932..
SHA256:	d9005fbd977fd39.
Tags:	AgentTesla DHL exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

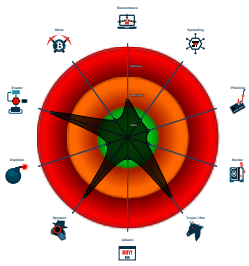
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Injects a PE file into a foreign proce…
- .NET source code contains very larg…
- Queries sensitive network adapter in…

Classification



Process Tree

- **System is w10x64**
- DHL - OVERDUE ACCOUNT - 130115482244.exe (PID: 1700 cmdline: "C:\Users\user\Desktop\DHL - OVERDUE ACCOUNT - 130115482244.exe" MD5: 3AADEBE9B94245452D74C655B2F04C0D)
  - DHL - OVERDUE ACCOUNT - 130115482244.exe (PID: 6220 cmdline: C:\Users\user\Desktop\DHL - OVERDUE ACCOUNT - 130115482244.exe MD5: 3AADEBE9B94245452D74C655B2F04C0D)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "ventas@mftecnologia.com.uy",
  "Password": "Ventas.1",
  "Host": "us2.smtp.mailhostbox.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000000.420640504.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000000.420640504.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.644568588.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.644568588.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000000.419459827.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.0.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.0.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.0.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32ae4:$s10: logins • 0x3254b:$s11: credential • 0x2eb48:$g1: get_Clipboard • 0x2eb56:$g2: get_Keyboard • 0x2eb63:$g3: get_Password • 0x2fe40:$g4: get_CtrlKeyDown • 0x2fe50:$g5: get_ShiftKeyDown • 0x2fe61:$g6: get_AltKeyDown
0.2.DHL - OVERDUE ACCOUNT - 130115482244.exe.42afe68.7.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.DHL - OVERDUE ACCOUNT - 130115482244.exe.42afe68.7.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 33 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to harvest and steal browser information (history, passwords, etc)

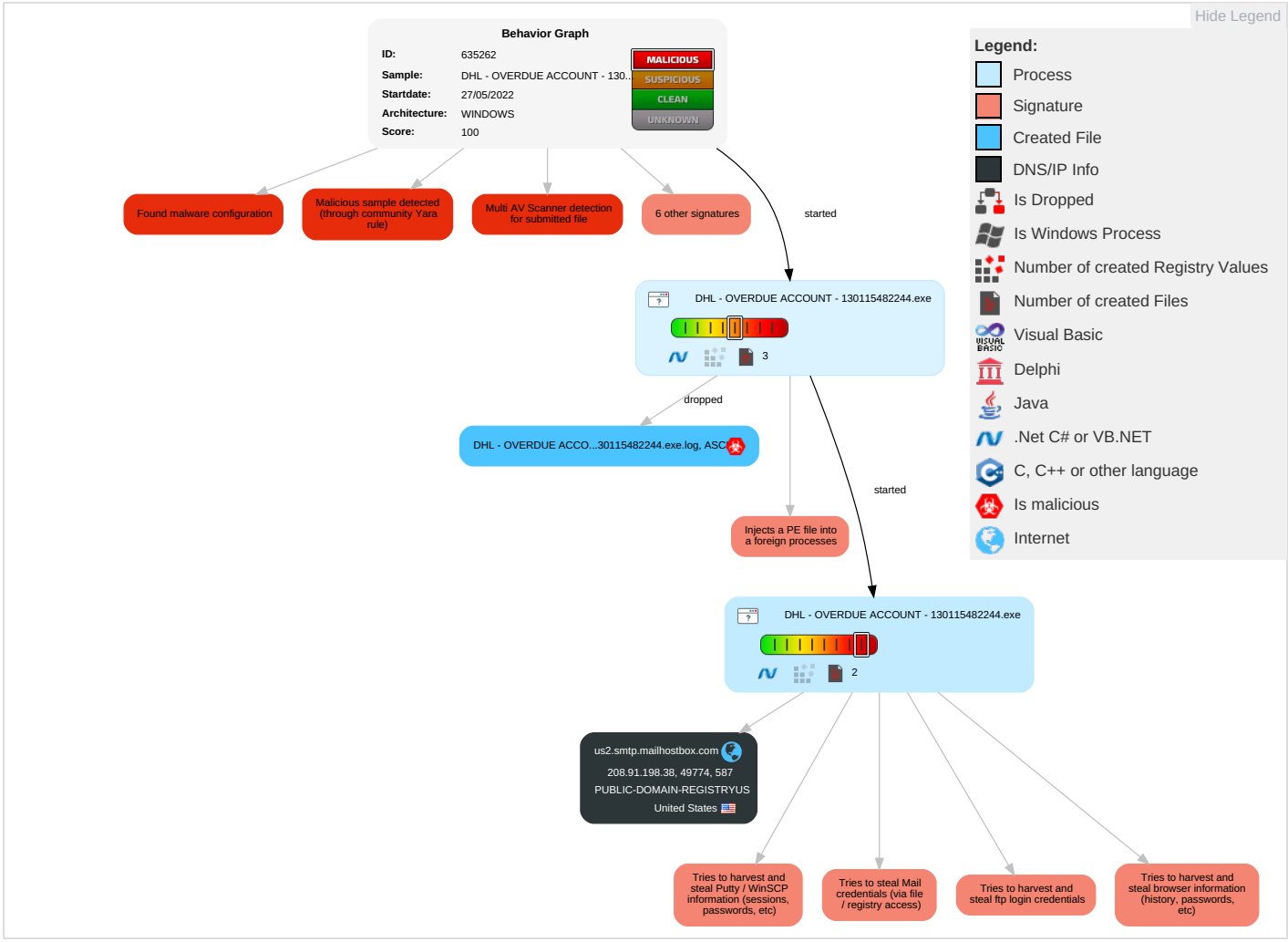
Remote Access Functionality

Yara detected AgentTesla

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	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	2 OS Credential Dumping	2 1 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	1 Input Capture	1 Process Discovery	Remote Desktop Protocol	1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 1 Archive Collected Data	Automated Exfiltration	1 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)	1 1 1 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	2 Data from Local System	Scheduled Transfer	1 1 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 Remote System Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 1 4 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 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

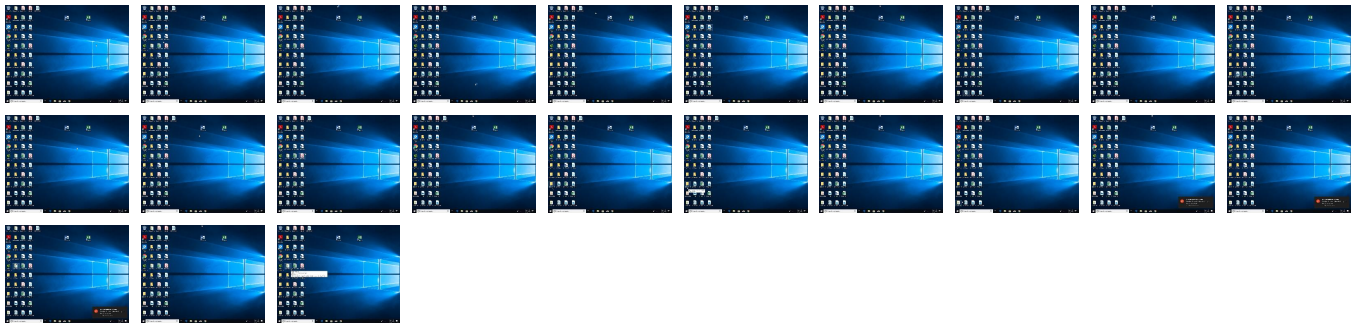
Behavior Graph



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 - OVERDUE ACCOUNT - 130115482244.exe	33%	Virustotal		Browse
DHL - OVERDUE ACCOUNT - 130115482244.exe	20%	ReversingLabs	ByteCode-MSIL.Spyware.Negasteal	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.2.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
1.0.DHL - OVERDUE ACCOUNT - 130115482244.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.com_/	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://EBusCZ.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://gmhwAFOW85IGv.org	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.198.38	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646099485.000000001751000.00000004.00000020.00020000.00000000.sdmp, DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.647118757.000000000354D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646349174.000000003201000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.apache.org/licenses/LICENSE-2.0	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designersG	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com/dcoetzee/plants-vs-zombies-user-file-editor	DHL - OVERDUE ACCOUNT - 130115482244.exe	false		high
http://https://sectigo.com/CPS0	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646099485.0000000001751000.00000004.00000020.00020000.00000000.sdmp, DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.647118757.000000000354D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.647118757.000000000354D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers?	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://github.com	DHL - OVERDUE ACCOUNT - 130115482244.exe	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646349174.0000000003201000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.tiro.com	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.423839638.0000000001817000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com_/	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.423839638.0000000001817000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.comgrita	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.423839638.0000000001817000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://EBusCZ.com	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646349174.0000000003201000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646349174.0000000003201000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ocsp.sectigo.com0A	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646099485.0000000001751000.00000004.00000020.00020000.00000000.sdmp, DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.647118757.000000000354D000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fonts.com	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://gmhwAFOW85IGv.org	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646980534.0000000003543000.00000004.00000800.00020000.00000000.sdmp, DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000001.00000002.646855464.0000000003513000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sakkal.com	DHL - OVERDUE ACCOUNT - 130115482244.exe, 00000000.00000002.430878005.0000000007302000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.198.38	us2.smtp.mailhostbox.com	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635262
Start date and time: 27/05/202218:03:41	2022-05-27 18:03:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL - OVERDUE ACCOUNT - 130115482244.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:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/1@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:05:07	API Interceptor	655x Sleep call for process: DHL - OVERDUE ACCOUNT - 130115482244.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL - OVERDUE ACCOUNT - 130115482244.exe.log

Process:	C:\Users\user\Desktop\DHL - OVERDUE ACCOUNT - 130115482244.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false

SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.754894395538076
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	DHL - OVERDUE ACCOUNT - 130115482244.exe
File size:	747520
MD5:	3aadebe9b94245452d74c655b2f04c0d
SHA1:	794dc763ca693288850d9a8ab73848d8146e19a7
SHA256:	d9005fbd977fd39146b129fb7e391765242be7857ba9dd921dc59339ce90d06d
SHA512:	976410c61688b601945b0c1af8c56dcee7c27726060349eefbfc068a1c66524c17a21a83529ce70d31662cbecba482e8e0fb6fc564b876db42a5990a2a45191c
SSDEEP:	12288:ui782P9bHoAUgvqVBgbAj/ExhYs6sQ9szP+x1gGvZZtKIMolhR8rf7oHUdvp8+Ki:ht1bHoHgbAj/Exhb6v9szM11vZZ0IM6E
TLSH:	3CF4F110B1F80F22E6BA57FD6570518407B67DA96520E38E1CD17CDB36B1F918A82F2B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...,J.b.....0.....Z.....*... ...@....@.. .....@.....

File Icon

Icon Hash:	4462f276dcec30e6

Static PE Info

General

Entrypoint:	0x4b2ae2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62904A2C [Fri May 27 03:49:00 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0

Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xb2a90	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xb4000	0x57e4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xba000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xb2958	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xb0ae8	0xb0c00	False	0.865699865187	data	7.75351668715	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xb4000	0x57e4	0x5800	False	0.965198863636	data	7.89347639679	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xba000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xb4100	0x51a3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xb92b4	0x14	data		
RT_VERSION	0xb92d8	0x30c	data		
RT_MANIFEST	0xb95f4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

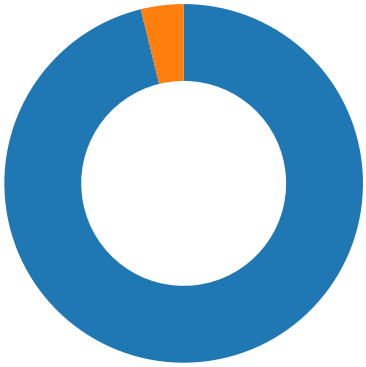
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	BadImageFormatExcept.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	BadImageFormatExcept.exe

Network Behavior

Network Port Distribution

Total Packets: 26

- 53 (DNS)
- 587 undefined



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:05:28.091377020 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:28.298784971 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:28.298952103 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:29.684762955 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:29.703710079 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:29.911066055 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:29.911160946 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:29.967134953 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:30.174669981 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:30.285147905 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:30.493076086 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:30.493102074 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:30.493119001 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:30.493133068 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:30.493180037 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:30.493227959 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:30.496767998 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:30.631525993 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:30.700508118 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:30.803258896 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:31.011755943 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:31.225344896 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:31.911557913 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:32.119132042 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:32.164371967 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:32.372899055 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:32.522336006 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:33.591638088 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:33.801672935 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:33.818130970 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:34.028259039 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:34.028717995 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:34.259850025 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:34.260349989 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:34.469849110 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:34.471039057 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:34.471165895 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:34.471879959 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:34.471966028 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:05:34.678272009 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:34.678913116 CEST	587	49774	208.91.198.38	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:05:34.827351093 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:05:35.022630930 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:07:07.958949089 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:07:08.166745901 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:07:08.167220116 CEST	587	49774	208.91.198.38	192.168.2.6
May 27, 2022 18:07:08.167516947 CEST	49774	587	192.168.2.6	208.91.198.38
May 27, 2022 18:07:08.170008898 CEST	49774	587	192.168.2.6	208.91.198.38

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:05:28.023284912 CEST	60350	53	192.168.2.6	8.8.8.8
May 27, 2022 18:05:28.046868086 CEST	53	60350	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:05:28.023284912 CEST	192.168.2.6	8.8.8.8	0xcd53	Standard query (0)	us2.smtp.mailhostbox.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:05:28.046868086 CEST	8.8.8.8	192.168.2.6	0xcd53	No error (0)	us2.smtp.mailhostbox.com		208.91.198.38	A (IP address)	IN (0x0001)
May 27, 2022 18:05:28.046868086 CEST	8.8.8.8	192.168.2.6	0xcd53	No error (0)	us2.smtp.mailhostbox.com		208.91.198.46	A (IP address)	IN (0x0001)
May 27, 2022 18:05:28.046868086 CEST	8.8.8.8	192.168.2.6	0xcd53	No error (0)	us2.smtp.mailhostbox.com		162.222.225.29	A (IP address)	IN (0x0001)
May 27, 2022 18:05:28.046868086 CEST	8.8.8.8	192.168.2.6	0xcd53	No error (0)	us2.smtp.mailhostbox.com		162.222.225.16	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 18:05:29.684762955 CEST	587	49774	208.91.198.38	192.168.2.6	220 us2.outbound.mailhostbox.com ESMTP Postfix
May 27, 2022 18:05:29.703710079 CEST	49774	587	192.168.2.6	208.91.198.38	EHLO 134349
May 27, 2022 18:05:29.911160946 CEST	587	49774	208.91.198.38	192.168.2.6	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-DSN 250 CHUNKING
May 27, 2022 18:05:29.967134953 CEST	49774	587	192.168.2.6	208.91.198.38	STARTTLS
May 27, 2022 18:05:30.174669981 CEST	587	49774	208.91.198.38	192.168.2.6	220 2.0.0 Ready to start TLS

Statistics

Behavior

● DHL - OVERDUE ACCOUNT - 1301.
● DHL - OVERDUE ACCOUNT - 1301.

Click to jump to process

System Behavior

Analysis Process: DHL - OVERDUE ACCOUNT - 130115482244.exe PID: 1700, Parent PID: 1592

General

Target ID:	0
Start time:	18:04:55
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DHL - OVERDUE ACCOUNT - 130115482244.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL - OVERDUE ACCOUNT - 130115482244.exe"
Imagebase:	0xd90000
File size:	747520 bytes
MD5 hash:	3AADEBE9B94245452D74C655B2F04C0D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.433764816.0000000007A40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.424115228.00000000031A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.425042726.0000000003270000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.428041708.0000000004279000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.428041708.0000000004279000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC2CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL - OVERDUE ACCOUNT - 130115482244.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DF3C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL - OVERDUE ACCOUNT - 130115482244.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DF3C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA71B4F	ReadFile

Analysis Process: DHL - OVERDUE ACCOUNT - 130115482244.exe PID: **6220**, Parent PID: **1700**

General

Target ID:	1
Start time:	18:05:15
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DHL - OVERDUE ACCOUNT - 130115482244.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL - OVERDUE ACCOUNT - 130115482244.exe
Imagebase:	0xf00000
File size:	747520 bytes
MD5 hash:	3AADEBE9B94245452D74C655B2F04C0D
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.420640504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.420640504.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.644568588.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.644568588.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.419459827.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.419459827.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.420135063.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.420135063.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000000.418939154.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000000.418939154.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.646349174.0000000003201000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.646349174.0000000003201000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC2CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DC2CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DC05705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC0CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB603DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB603DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DC05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DC05705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CA71B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CA71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CA71B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\98bd75d2-ce84-459a-aada-2da99aef3201	unknown	4096	success or wait	1	6CA71B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11072	success or wait	1	6CA71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CA71B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CA71B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CA71B4F	ReadFile

Disassembly

No disassembly