ID: 339038
Sample Name: DHL document.exe
Cookbook: default.jbs
Time: 09:48:17
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

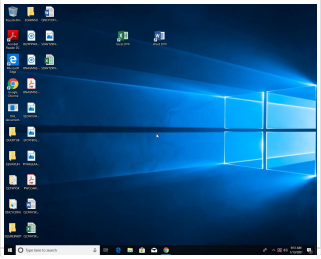
Analysis Report DHL document.exe

Overview

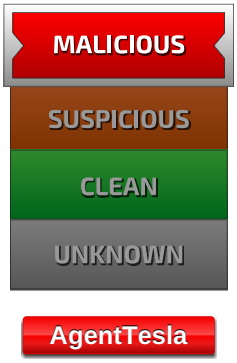
General Information

Sample Name:	DHL document.exe
Analysis ID:	339038
MD5:	5c629d2ad3a452..
SHA1:	8b32e938bcd05fb.
SHA256:	566554b534a531..
Tags:	AgentTesla DHL exe

Most interesting Screenshot:



Detection

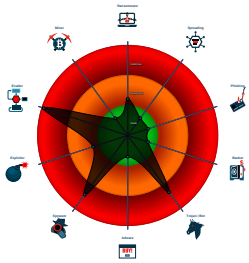


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Initial sample is a PE file and has a …
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- DHL document.exe (PID: 6756 cmdline: 'C:\Users\user\Desktop\DHL document.exe' MD5: 5C629D2AD3A45250EEBC832C568E9AD0)
  - DHL document.exe (PID: 7004 cmdline: {path} MD5: 5C629D2AD3A45250EEBC832C568E9AD0)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "pFchlRoNMUTKWto",
  "URL: ": "https://B2bQlilPZYn20R.org",
  "To: ": "nado@dicon.md",
  "ByHost: ": "mail.dicon.md:587",
  "Password: ": "dVALs",
  "From: ": "nado@dicon.md"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.236255563.000000000336 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000002.00000002.587585011.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.593469319.0000000002B1 1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.593469319.0000000002B1 1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.238800439.0000000004D4 6000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 3 entries				

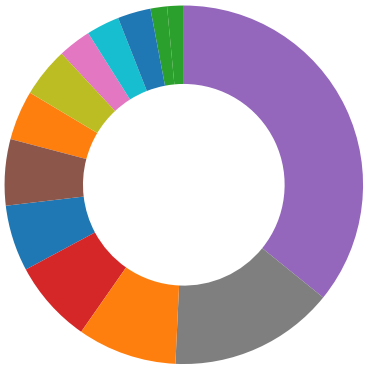
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.DHL document.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

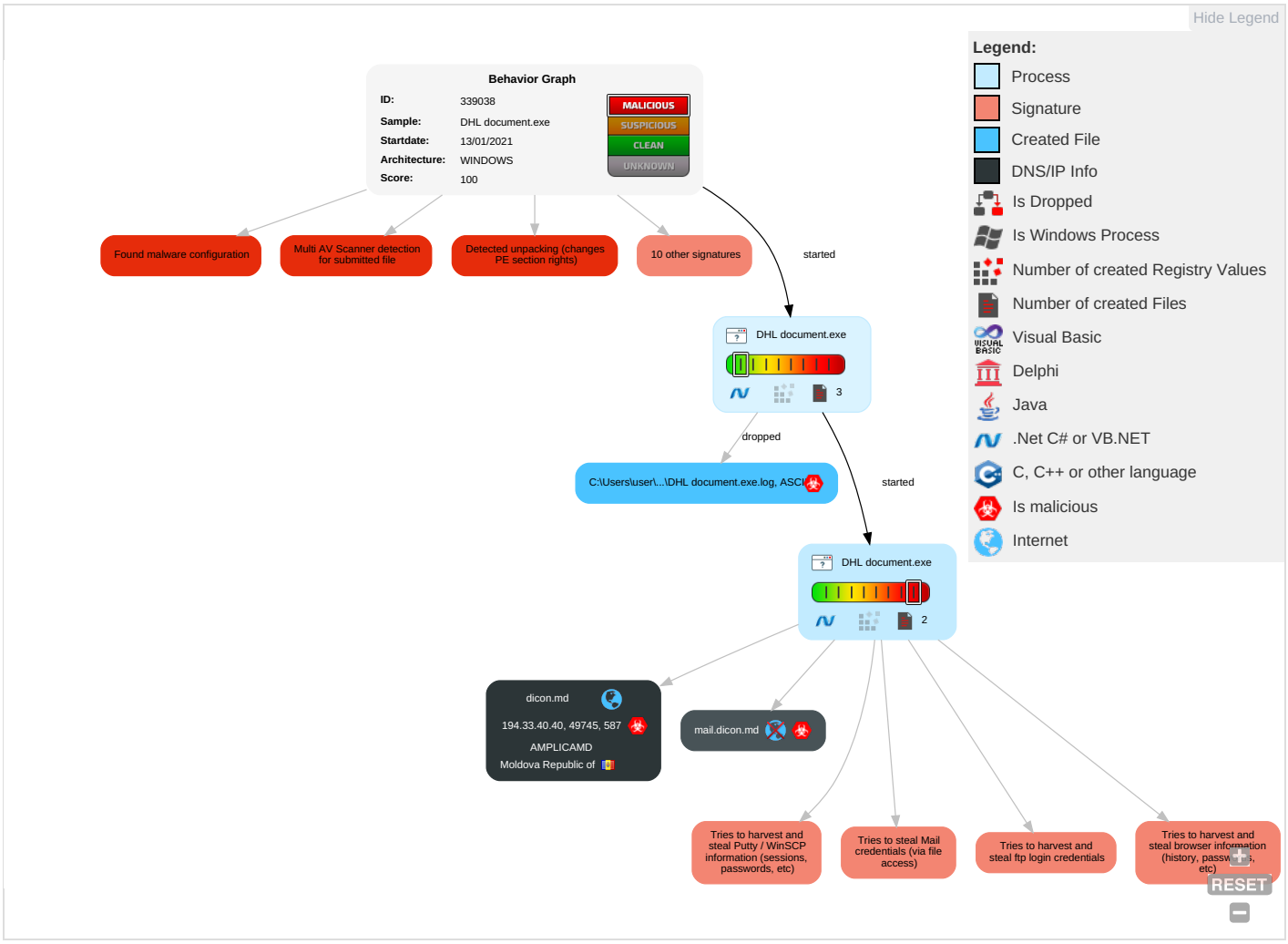
Remote Access Functionality:

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
Valid Accounts	Windows Management Instrumentation 2 1 1	Path Interception	Process Injection 1 2	Masquerading 1	OS Credential Dumping 2	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 3	Credentials in Registry 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Data from Local System 2	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 3	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 2 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

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 document.exe	39%	Virustotal		Browse
DHL document.exe	23%	ReversingLabs	Win32.Trojan.Pwsx	
DHL document.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.DHL document.exe.f20000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
2.2.DHL document.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
dicon.md	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://B2bQlilPZYn20R.org	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-d	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://stPqVp.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/-cz	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://r3.o.lencr.Dll	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cnq	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgreta	0%	Avira URL Cloud	safe	
http://r3.i.lencr.org/05	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Tpq	0%	Avira URL Cloud	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://r3.o.lencr.org0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/=	0%	Avira URL Cloud	safe	
http://r3.o.lencr.D	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://dicon.md	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/q	0%	Avira URL Cloud	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://mail.dicon.md	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/tion	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dicon.md	194.33.40.40	true	true	• 0%, Virustotal, Browse	unknown
mail.dicon.md	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://B2bQlilPZYn20R.org	true	• Avira URL Cloud: safe	unknown

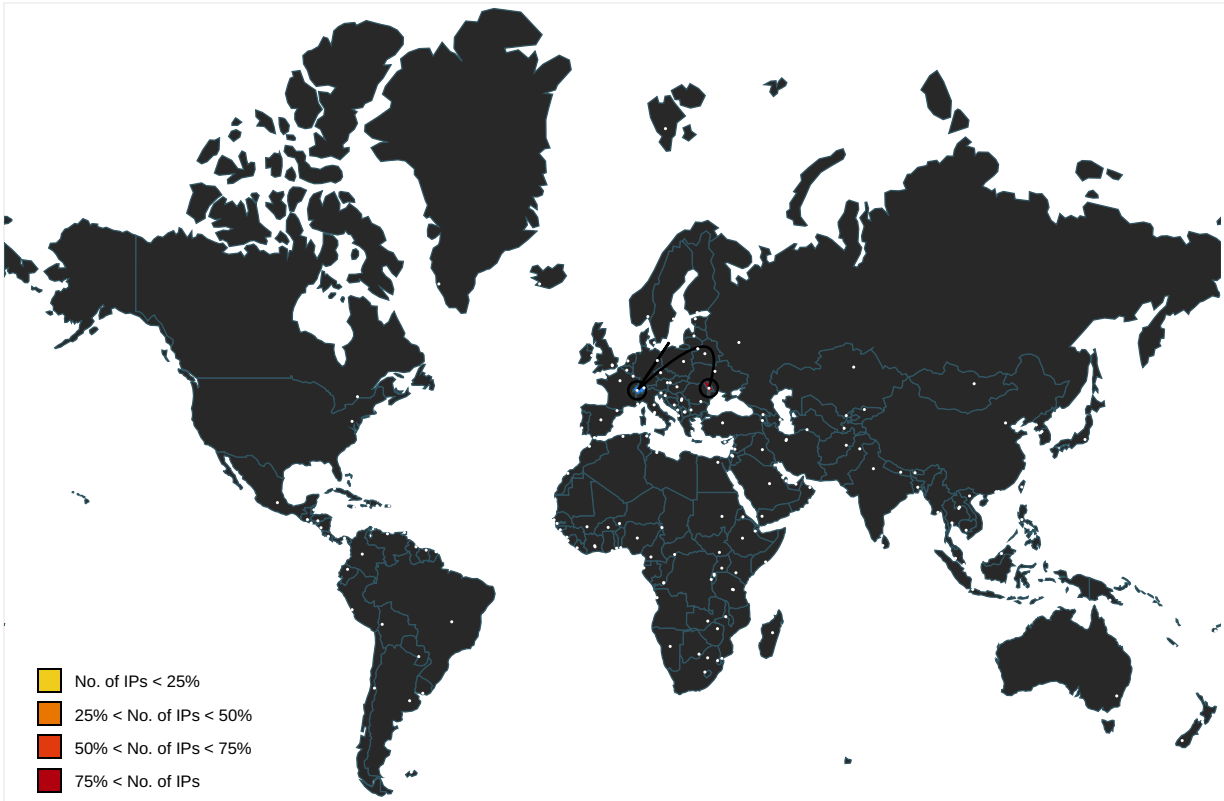
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	DHL document.exe, 00000002.00000002.593469319.0000000002B11000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	DHL document.exe, 00000000.00000002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	DHL document.exe, 00000000.00000002.245898824.00000000088000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/a-d	DHL document.exe, 00000000.00003.216784260.000000000871B0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://stPqVp.com	DHL document.exe, 00000002.00002.593469319.0000000002B110.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/-cz	DHL document.exe, 00000000.00003.216960659.000000000871B0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://r3.o.lencr.Dll	DHL document.exe, 00000002.00002.600615092.00000000066B00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cnq	DHL document.exe, 00000000.00003.215386674.00000000087210.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comgreta	DHL document.exe, 00000000.00002.245870053.000000000871A0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.i.lencr.org/05	DHL document.exe, 00000002.00002.596699160.0000000002E260.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/Tpq	DHL document.exe, 00000000.00003.216784260.000000000871B0.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.org0	DHL document.exe, 00000002.00002.596699160.0000000002E260.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fonts.com	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false		high
http://www.sandoll.co.kr	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	DHL document.exe, 00000000.00002.245898824.00000000088000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	DHL document.exe, 00000002.00002.587585011.00000000004020.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://cps.root-x1.letsencrypt.org0	DHL document.exe, 00000002.00000002.596699160.0000000002E26000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	DHL document.exe, 00000002.00000002.593469319.0000000002B11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.letsencrypt.org0	DHL document.exe, 00000002.00000002.596699160.0000000002E26000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	DHL document.exe, 00000002.00000002.593469319.0000000002B11000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/N	DHL document.exe, 00000000.00000003.216960659.000000000871B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/=	DHL document.exe, 00000000.00000003.215701958.0000000008722000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://r3.o.lencr.D	DHL document.exe, 00000002.00000002.600615092.00000000066B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	DHL document.exe, 00000000.00000003.216960659.000000000871B000.00000004.00000001.sdmp, DHL document.exe, 00000000.00000003.217255637.000000000871B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.coml	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.founder.com.cn/cn/	DHL document.exe, 00000000.00000003.215832766.0000000008723000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false		high
http://dicon.md	DHL document.exe, 00000002.00000002.596699160.0000000002E26000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Y0/	DHL document.exe, 00000000.00000003.216960659.000000000871B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/q	DHL document.exe, 00000000.00000003.216960659.000000000871B000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.monotype.	DHL document.exe, 00000000.00000003.217557117.0000000008722000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comm	DHL document.exe, 00000000.00000002.245870053.000000000871A000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	DHL document.exe, 00000000.00000003.216960659.000000000871B000.00000004.00000001.sdmp, DHL document.exe, 00000000.00000003.216486611.0000000008713000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.dicon.md	DHL document.exe, 00000002.00000002.596699160.0000000002E26000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers8	DHL document.exe, 00000000.00000002.245898824.0000000008800000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/tion	DHL document.exe, 00000000.00000003.216486611.0000000008713000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.33.40.40	unknown	Moldova Republic of		206698	AMPLICAMD	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339038
Start date:	13.01.2021
Start time:	09:48:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL document.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:	28
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@2/1

EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.2% (good quality ratio 0.6%) • Quality average: 32.9% • Quality standard deviation: 37.7%
HCA Information:	• Successful, ratio: 93% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 40.88.32.150, 104.43.193.48, 92.122.144.200, 51.11.168.160, 92.122.213.194, 92.122.213.247, 8.248.139.254, 67.26.81.254, 8.248.113.254, 67.27.157.254, 8.248.135.254, 51.103.5.186, 20.54.26.129, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, wns.notify.windows.com.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, par02p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net • 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
09:49:16	API Interceptor	1089x Sleep call for process: DHL document.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.33.40.40	DHL Tracking.exe	Get hash	malicious	Browse	
	DHL fill.exe	Get hash	malicious	Browse	
	BL FOR SHIPMENT_doc.gz.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMPLICAMD	DHL Tracking.exe	Get hash	malicious	Browse	• 194.33.40.40
	DHL fill.exe	Get hash	malicious	Browse	• 194.33.40.40
	BL FOR SHIPMENT_doc.gz.exe	Get hash	malicious	Browse	• 194.33.40.40
	15#U043e #U0437#U0430#U043a#U0430#U0437#U0435.js	Get hash	malicious	Browse	• 185.165.242.5

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL document.exe.log	
Process:	C:\Users\user\Desktop\DHL document.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
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):	7.450519577624797

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHL document.exe
File size:	1092608
MD5:	5c629d2ad3a45250eebc832c568e9ad0
SHA1:	8b32e938bcd05fb40ec673607a4748b4badbd614
SHA256:	566554b534a53102dd67fc20bd07ca49241b51616d73619e383e80bdfc4fe08a
SHA512:	311a877d39f6edab27162139a9ac0517a60284725a8c766d00a81b4d786fa0b59d4c5dd88d6cf873be5b6170d3a2a4ce5c61e30926b3c0a27e20b2abf155c1a4
SSDEEP:	24576:hve37f8hNMvbH4NvcP7MEv73i3DiTsRt1GKtijAHk0+QWO:teD8hNMjNQEbi3WE1GNjAHkg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....0._.....0.....n.... ....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50bf6e
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:	0x5FFE3011 [Tue Jan 12 23:26:09 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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
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 al, byte ptr [eax]
adc byte ptr [eax], al
add byte ptr [eax], al
and byte ptr [eax], al
add byte ptr [eax+00000018h], al
push eax
add byte ptr [eax], al
add byte ptr [eax], 00000000h
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 dword ptr [eax], eax
add dword ptr [eax], eax
add byte ptr [eax], al
cmp byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x10bf1c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10c000	0x618	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x109f74	0x10a000	False	0.759986820078	data	7.45714176103	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10c000	0x618	0x800	False	0.33251953125	data	3.4919599184	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10e000	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_VERSION	0x10c0a0	0x388	data		
RT_MANIFEST	0x10c428	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

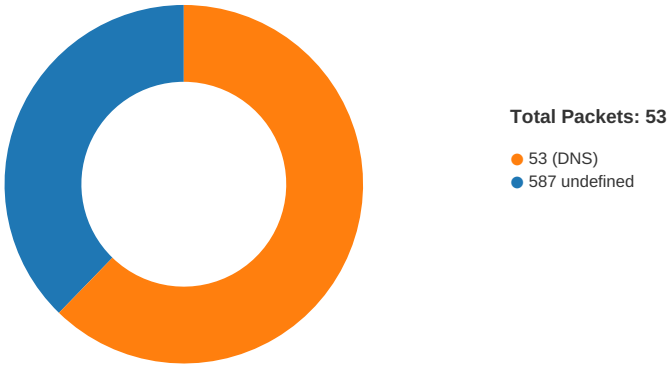
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright Overwolf 2011 - 2020
Assembly Version	2.159.0.0
InternalName	q.exe
FileVersion	2.159.0.0
CompanyName	Overwolf Ltd.
LegalTrademarks	
Comments	Overwolf Launcher
ProductName	OverwolfLauncher
ProductVersion	2.159.0.0
FileDescription	OverwolfLauncher
OriginalFilename	q.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 09:51:01.825942993 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:01.902034044 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:01.902193069 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.108988047 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.109482050 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.185610056 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.186029911 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.267008066 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.309504032 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.349914074 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.444653988 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.444685936 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.444696903 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.444849014 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.452533007 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.529319048 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.575144053 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.757524014 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.834646940 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.836457968 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:02.912600040 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:02.913161993 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:03.003572941 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.004545927 CET	49745	587	192.168.2.3	194.33.40.40

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 09:51:03.080638885 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.081073999 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:03.157834053 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.158317089 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:03.234335899 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.237036943 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:03.237193108 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:03.237718105 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:03.237828970 CET	49745	587	192.168.2.3	194.33.40.40
Jan 13, 2021 09:51:03.313261986 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.313291073 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.313767910 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.314073086 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.543636084 CET	587	49745	194.33.40.40	192.168.2.3
Jan 13, 2021 09:51:03.590858936 CET	49745	587	192.168.2.3	194.33.40.40

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 09:49:03.694417000 CET	60100	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:03.745235920 CET	53	60100	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:04.610464096 CET	53195	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:04.658298969 CET	53	53195	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:05.386686087 CET	50141	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:05.437436104 CET	53	50141	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:06.375423908 CET	53023	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:06.423270941 CET	53	53023	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:07.369059086 CET	49563	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:07.417152882 CET	53	49563	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:08.194067955 CET	51352	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:08.241970062 CET	53	51352	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:09.458926916 CET	59349	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:09.506897926 CET	53	59349	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:10.713337898 CET	57084	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:10.761334896 CET	53	57084	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:11.676616907 CET	58823	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:11.724546909 CET	53	58823	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:12.676824093 CET	57568	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:12.724822044 CET	53	57568	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:13.685590982 CET	50540	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:13.736304045 CET	53	50540	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:34.834316969 CET	54366	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:34.892573118 CET	53	54366	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:35.449153900 CET	53034	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:35.497189045 CET	53	53034	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:41.908828020 CET	57762	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:41.966502905 CET	53	57762	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:53.200333118 CET	55435	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:53.256689072 CET	53	55435	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:53.524684906 CET	50713	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:53.583791971 CET	53	50713	8.8.8.8	192.168.2.3
Jan 13, 2021 09:49:58.342025042 CET	56132	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:49:58.402996063 CET	53	56132	8.8.8.8	192.168.2.3
Jan 13, 2021 09:50:01.186121941 CET	58987	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:50:01.250853062 CET	53	58987	8.8.8.8	192.168.2.3
Jan 13, 2021 09:50:31.712558985 CET	56579	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:50:31.760452032 CET	53	56579	8.8.8.8	192.168.2.3
Jan 13, 2021 09:50:32.170082092 CET	60633	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:50:32.234213114 CET	53	60633	8.8.8.8	192.168.2.3
Jan 13, 2021 09:50:54.551919937 CET	61292	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:50:54.600152969 CET	53	61292	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:01.497750998 CET	63619	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:51:01.599282980 CET	53	63619	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:01.614475965 CET	64938	53	192.168.2.3	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 09:51:01.716131926 CET	53	64938	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:55.506907940 CET	61946	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:51:55.566407919 CET	53	61946	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:56.407442093 CET	64910	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:51:56.463999987 CET	53	64910	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:57.180030107 CET	52123	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:51:57.239193916 CET	53	52123	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:57.686512947 CET	56130	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:51:57.745301962 CET	53	56130	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:58.330986977 CET	56338	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:51:58.389489889 CET	53	56338	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:59.010564089 CET	59420	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:51:59.058460951 CET	53	59420	8.8.8.8	192.168.2.3
Jan 13, 2021 09:51:59.935642004 CET	58784	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:51:59.992357969 CET	53	58784	8.8.8.8	192.168.2.3
Jan 13, 2021 09:52:01.043257952 CET	63978	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:52:01.100410938 CET	53	63978	8.8.8.8	192.168.2.3
Jan 13, 2021 09:52:02.250788927 CET	62938	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:52:02.310050964 CET	53	62938	8.8.8.8	192.168.2.3
Jan 13, 2021 09:52:03.387768984 CET	55708	53	192.168.2.3	8.8.8.8
Jan 13, 2021 09:52:03.444245100 CET	53	55708	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 09:51:01.497750998 CET	192.168.2.3	8.8.8.8	0x6fff	Standard query (0)	mail.dicon.md	A (IP address)	IN (0x0001)
Jan 13, 2021 09:51:01.614475965 CET	192.168.2.3	8.8.8.8	0xd98d	Standard query (0)	mail.dicon.md	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 09:51:01.599282980 CET	8.8.8.8	192.168.2.3	0x6fff	No error (0)	mail.dicon.md	dicon.md		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 09:51:01.599282980 CET	8.8.8.8	192.168.2.3	0x6fff	No error (0)	dicon.md		194.33.40.40	A (IP address)	IN (0x0001)
Jan 13, 2021 09:51:01.716131926 CET	8.8.8.8	192.168.2.3	0xd98d	No error (0)	mail.dicon.md	dicon.md		CNAME (Canonical name)	IN (0x0001)
Jan 13, 2021 09:51:01.716131926 CET	8.8.8.8	192.168.2.3	0xd98d	No error (0)	dicon.md		194.33.40.40	A (IP address)	IN (0x0001)

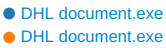
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 13, 2021 09:51:02.108988047 CET	587	49745	194.33.40.40	192.168.2.3	220-web2.amplica.net ESMTP Exim 4.93 #2 Wed, 13 Jan 2021 10:51:02 +0200 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jan 13, 2021 09:51:02.109482050 CET	49745	587	192.168.2.3	194.33.40.40	EHLO 414408
Jan 13, 2021 09:51:02.185610056 CET	587	49745	194.33.40.40	192.168.2.3	250-web2.amplica.net Hello 414408 [84.17.52.74] 250-SIZE 83886080 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Jan 13, 2021 09:51:02.186029911 CET	49745	587	192.168.2.3	194.33.40.40	STARTTLS
Jan 13, 2021 09:51:02.267008066 CET	587	49745	194.33.40.40	192.168.2.3	220 TLS go ahead

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: DHL document.exe PID: 6756 Parent PID: 5596

General

Start time:	09:49:08
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\DHL document.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL document.exe'
Imagebase:	0xf20000
File size:	1092608 bytes
MD5 hash:	5C629D2AD3A45250EEBC832C568E9AD0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.236255563.0000000003361000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.238800439.0000000004D46000.00000004.00000001.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	6DEECF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	6DEECF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL document.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1FC78D	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 document.exe.log	unknown	1216	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",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_v4.0.3	success or wait	1	6E1FC907	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile

Analysis Process: DHL document.exe PID: 7004 Parent PID: 6756

General

Start time:	09:49:20
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\DHL document.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4e0000
File size:	1092608 bytes
MD5 hash:	5C629D2AD3A45250EEBC832C568E9AD0
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: 00000002.00000002.587585011.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.593469319.0000000002B11000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.593469319.0000000002B11000.00000004.00000001.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	6DEECF06	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	6DEECF06	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	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEC5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DECCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\6d7b2c83-aa9e-4828-bcff-140835a76c17	unknown	4096	success or wait	1	6CD31B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CD31B4F	ReadFile

Disassembly

Code Analysis