ID: 635261
Sample Name: DHL DELIVERY.exe
Cookbook: default.jbs
Time: 18:03:22
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

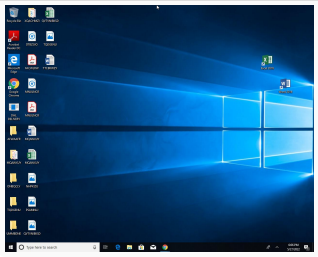
Windows Analysis Report

DHL DELIVERY.exe

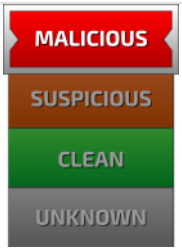
Overview

General Information

Sample Name:	DHL DELIVERY.exe
Analysis ID:	635261
MD5:	56a08fd913bfc20..
SHA1:	b135f9c44b2847..
SHA256:	37305d441b0332..
Tags:	AgentTesla DHL exe
Infos:	



Detection



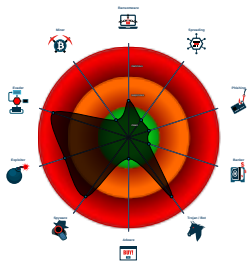
AgentTesla

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

Signatures

- Found malware configuration
- Yara detected UAC Bypass using C…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…
- Contains functionality to hide user a…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- DHL DELIVERY.exe (PID: 6860 cmdline: "C:\Users\user\Desktop\DHL DELIVERY.exe" MD5: 56A08FD913BFC20FA0F15A4FB204BAC9)
  - DHL DELIVERY.exe (PID: 6984 cmdline: C:\Users\user\Desktop\DHL DELIVERY.exe MD5: 56A08FD913BFC20FA0F15A4FB204BAC9)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "amycarrol@cobinparkop.com",
  "Password": "WLhpQ58eJQHBZqb",
  "Host": "smtp.privateemail.com"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.692251401.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000002.692251401.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000000.463670113.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.463670113.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.464161754.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.DHL DELIVERY.exe.400000.12.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.DHL DELIVERY.exe.400000.12.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
3.0.DHL DELIVERY.exe.400000.12.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x32b07:$s10: logins • 0x3256e:$s11: credential • 0x2eb86:$g1: get_Clipboard • 0x2eb94:$g2: get_Keyboard • 0x2eba1:$g3: get_Password • 0x2fe7b:$g4: get_CtrlKeyDown • 0x2fe8b:$g5: get_ShiftKeyDown • 0x2fe9c:$g6: get_AltKeyDown
3.0.DHL DELIVERY.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
3.0.DHL DELIVERY.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 31 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Exploits

Yara detected UAC Bypass using CMSTP

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Hooking and other Techniques for Hiding and Protection

Contains functionality to hide user accounts

Malware Analysis System Evasion

Yara detected AntiVM3
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

.NET source code references suspicious native API functions

Stealing of Sensitive Information

Yara detected AgentTesla
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
Tries to harvest and steal ftp login credentials
Tries to harvest and steal browser information (history, passwords, etc)

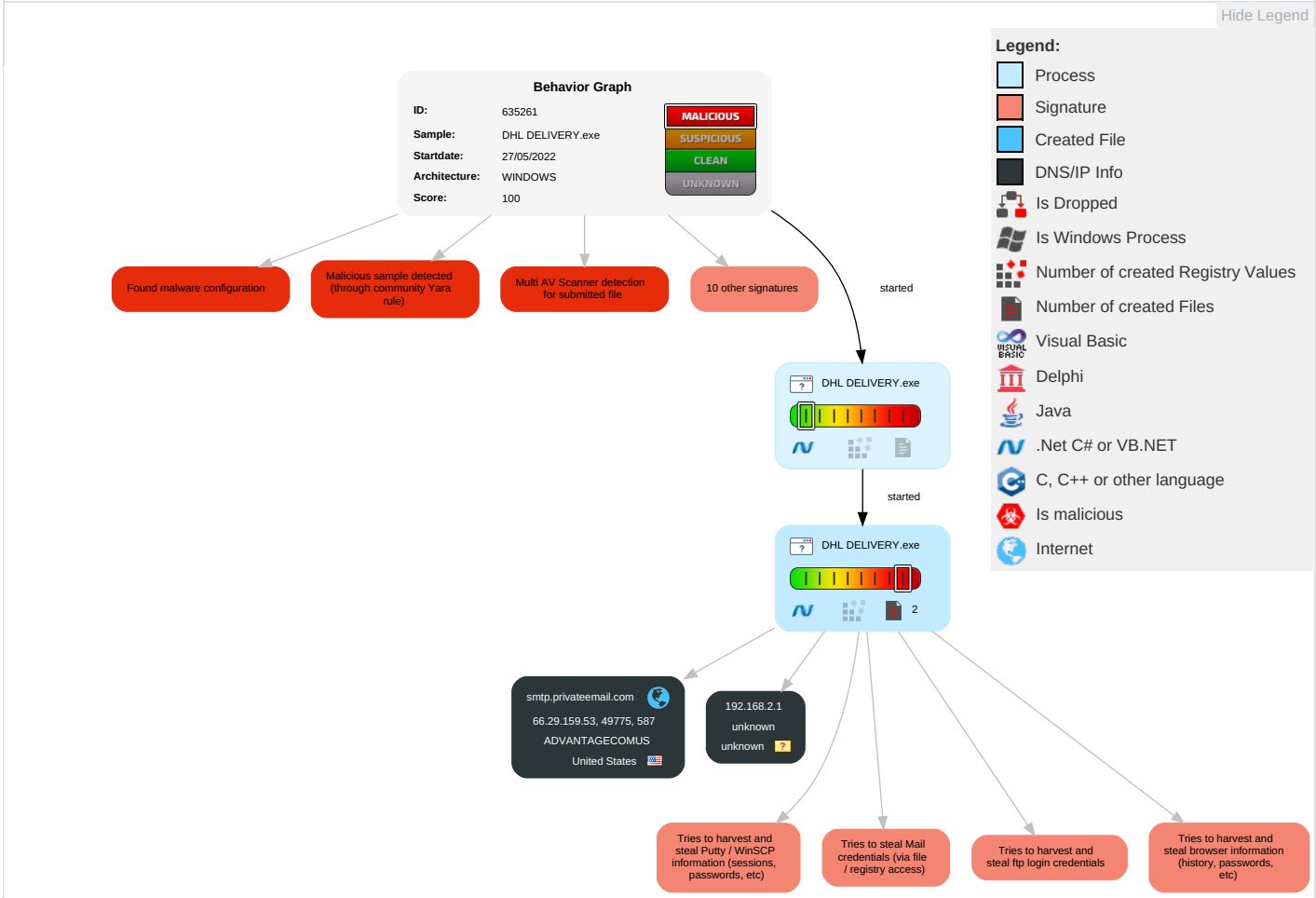
Remote Access Functionality

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 Query Registry	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 3 1 Virtualization/Sandbox Evasion	1 Credentials in Registry	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	2 Data from Local System	Automated Exfiltration	1 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 Deobfuscate/Decode Files or Information	NTDS	1 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Users	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	3 Obfuscated Files or Information	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	1 1 4 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

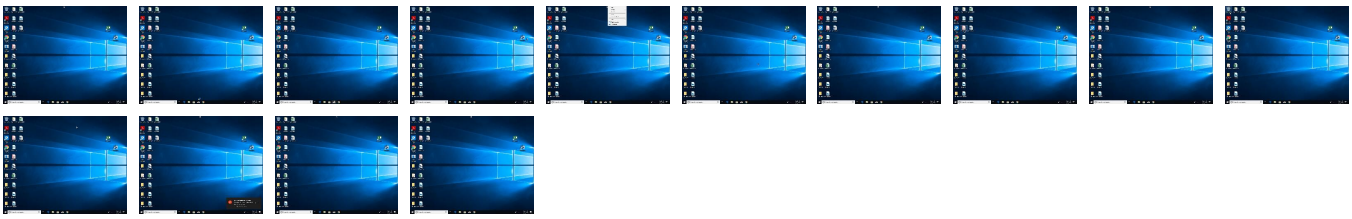
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL DELIVERY.exe	31%	Virustotal		Browse
DHL DELIVERY.exe	35%	ReversingLabs	ByteCode-MSIL.Trojan.Injuke	
DHL DELIVERY.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.DHL DELIVERY.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL DELIVERY.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL DELIVERY.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.DHL DELIVERY.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL DELIVERY.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.DHL DELIVERY.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://api.ipify.org%%startupfolder%	0%	URL Reputation	safe	
http://x2lvz0L9UI.com	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://fnqsTS.com	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

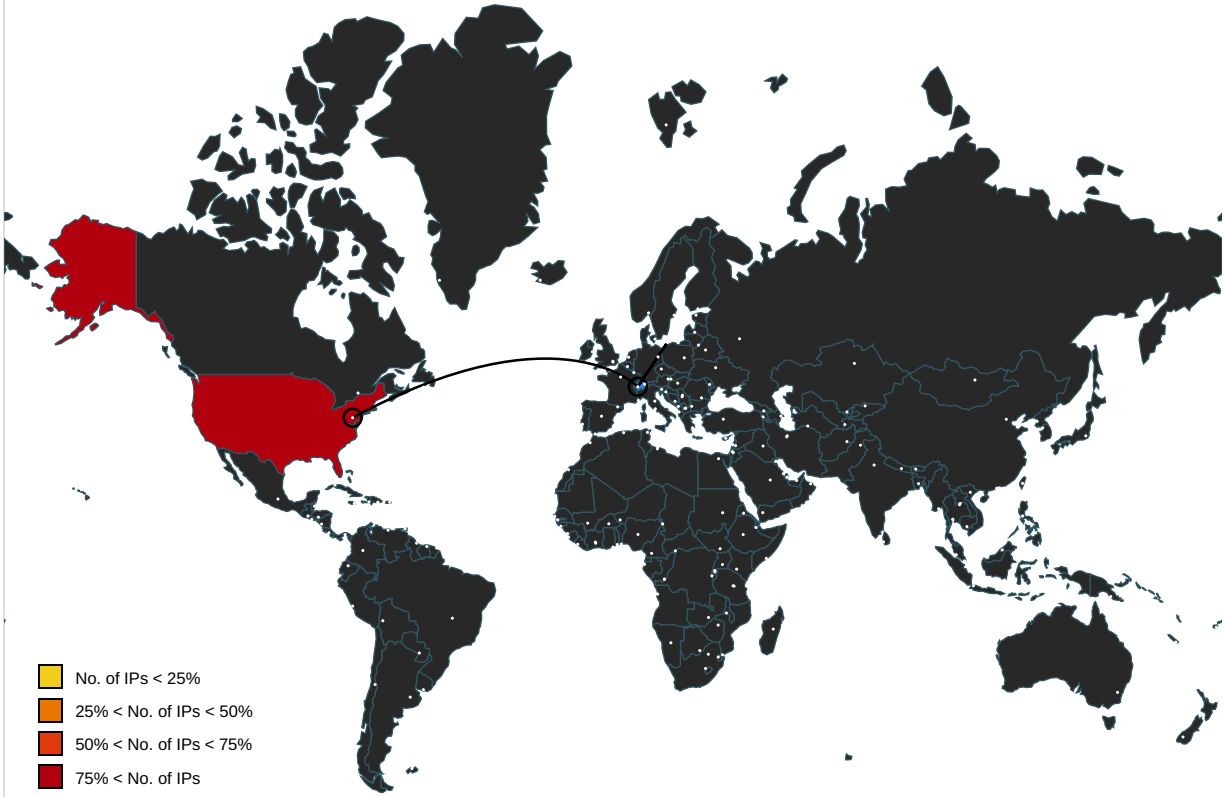
Name	IP	Active	Malicious	Antivirus Detection	Reputation
smtp.privateemail.com	66.29.159.53	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.random.org/sequences/	DHL DELIVERY.exe	false		high
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	DHL DELIVERY.exe, 00000003.00000002.696918969.0000000003476000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://127.0.0.1:HTTP/1.1	DHL DELIVERY.exe, 00000003.00000002.695721560.0000000003121000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://sectigo.com/CPS0	DHL DELIVERY.exe, 00000003.00000002.696918969.0000000003476000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%%startupfolder%	DHL DELIVERY.exe, 00000003.00000002.695721560.0000000003121000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://x2lvz0L9UI.com	DHL DELIVERY.exe, 00000003.00000002.695721560.0000000003121000.00000004.00000800.00020000.00000000.sdmp, DHL DELIVERY.exe, 00000003.00000002.697005706.00000000034A2000.00000004.00000800.00020000.00000000.sdmp, DHL DELIVERY.exe, 00000003.00000002.696995944.000000000349A000.00000004.00000800.00020000.00000000.sdmp, DHL DELIVERY.exe, 00000003.00000002.696902033.0000000003470000.00000004.00000800.00020000.00000000.sdmp, DHL DELIVERY.exe, 00000003.00000002.696858077.0000000003432000.00000004.00000800.00020000.00000000.sdmp, DHL DELIVERY.exe, 00000003.00000002.696885279.000000000346C000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.sectigo.com0	DHL DELIVERY.exe, 00000003.00000002.696918969.0000000003476000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fnqsTS.com	DHL DELIVERY.exe, 00000003.00000002.695721560.0000000003121000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://api.ipify.org%	DHL DELIVERY.exe, 00000003.00000002.695721560.0000000003121000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://smtp.privateemail.com	DHL DELIVERY.exe, 00000003.00000002.696918969.0000000003476000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	DHL DELIVERY.exe, 00000003.00000002.6957 21560.0000000003121000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNSnamejidpasswordPsi/Psi	DHL DELIVERY.exe, 00000003.00000002.6957 21560.0000000003121000.00000004.00000800 .00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
66.29.159.53	smtp.privateemail.com	United States		19538	ADVANTAGECOMUS	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635261
Start date and time: 27/05/202218:03:22	2022-05-27 18:03:22 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 34s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL DELIVERY.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:	21
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.expl.evad.winEXE@3/0@1/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.4% (good quality ratio 0.4%) • Quality average: 70.1% • Quality standard deviation: 24.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

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

Simulations

Behavior and APIs

Time	Type	Description
18:04:54	API Interceptor	713x Sleep call for process: DHL DELIVERY.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.907392354286095
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 DELIVERY.exe
File size:	574976
MD5:	56a08fd913bfc20fa0f15a4fb204bac9
SHA1:	b135f9c44b2847d494f1b2d843444711c8421cc0
SHA256:	37305d441b0332e9756a972f0585748807fb90ef363116aa6a224cefa120d09e
SHA512:	cae86e058d6416a72aaa97d5cb970a9cd12a21f65af1bee3ffe0924c787791b8f0366991a9fb0137e537e9226f06167cf5ac1c3cd1ab462615ea0a9bb0430f22
SSDEEP:	12288:KK2HUdEv8+F2wPLcYfqqDLNoE3TkyuFmcFiGZjC8Ng9n:KK2HrvY8zHNoCTkyuBFM8y
TLSH:	30C4129037B96F2BEA7E4EF98176106443B1B6066B50C3CE2DD276EE11E3F018E55A13
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...t.KR.....0.3...@.....-.... .....@.. ....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48db2d
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, HIGH_ENTROPY_VA
Time Stamp:	0x524B8F74 [Wed Oct 2 03:13:56 2013 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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8da4c	0x4a	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8e000	0x434	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x90000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x8da96	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
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

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x8bb33	0x8bc00	False	0.911831604987	data	7.9180819868	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8e000	0x434	0x600	False	0.305989583333	data	2.56725335834	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x90000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x8e058	0x3dc	data		

Imports

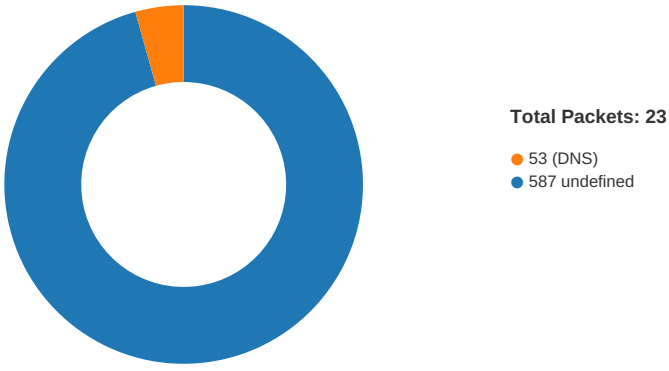
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Microsoft Corporation. All rights reserved.
Assembly Version	5.0.0.0
InternalName	System.Web.Cors.dll
FileVersion	5.0.11001.0
CompanyName	Microsoft Corporation.
ProductName	Microsoft ASP.NET MVC
ProductVersion	5.0.11001.0
FileDescription	System.Web.Cors (88a1bd8d3344b5df289577425c0314e7f521e88a)
OriginalFilename	System.Web.Cors.dll

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:05:02.151860952 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:02.321647882 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:02.321768999 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:02.493024111 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:02.493402958 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:02.662947893 CEST	587	49775	66.29.159.53	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:05:02.663575888 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:02.663954020 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:02.834335089 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:02.874758005 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:03.046480894 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.047969103 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.048019886 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.048053026 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.048080921 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:03.048084974 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.048115015 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.048130035 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:03.075139046 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:03.244549990 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.245537043 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.387064934 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:03.556396961 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.557019949 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.558290005 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:03.727574110 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.729589939 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.730511904 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:03.899827003 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.903959036 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:03.906023979 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:04.075403929 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.078903913 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.079385042 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:04.248735905 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.290292025 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.290813923 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:04.460079908 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.461122990 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.478138924 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:04.478338957 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:04.479090929 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:04.479360104 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:05:04.647291899 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.647352934 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.648190022 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.648361921 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.706700087 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:05:04.926225901 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:06:42.094340086 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:06:42.263477087 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:06:42.264010906 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:06:42.264039993 CEST	587	49775	66.29.159.53	192.168.2.5
May 27, 2022 18:06:42.264090061 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:06:42.266407967 CEST	49775	587	192.168.2.5	66.29.159.53
May 27, 2022 18:06:42.435457945 CEST	587	49775	66.29.159.53	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:05:02.100497961 CEST	53934	53	192.168.2.5	8.8.8.8
May 27, 2022 18:05:02.121862888 CEST	53	53934	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:05:02.100497961 CEST	192.168.2.5	8.8.8.8	0x9d0e	Standard query (0)	smtp.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

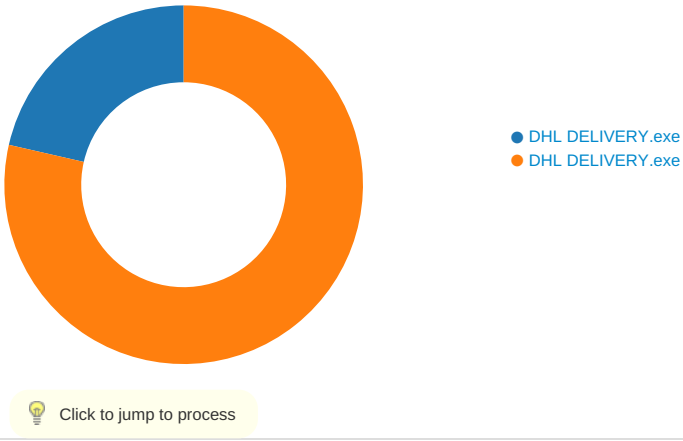
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:05:02.121862888 CEST	8.8.8.8	192.168.2.5	0x9d0e	No error (0)	smtp.privateemail.com		66.29.159.53	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
May 27, 2022 18:05:02.493024111 CEST	587	49775	66.29.159.53	192.168.2.5	220 PrivateEmail.com prod Mail Node
May 27, 2022 18:05:02.493402958 CEST	49775	587	192.168.2.5	66.29.159.53	EHLO 980108
May 27, 2022 18:05:02.663575888 CEST	587	49775	66.29.159.53	192.168.2.5	250-mta-08.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
May 27, 2022 18:05:02.663954020 CEST	49775	587	192.168.2.5	66.29.159.53	STARTTLS
May 27, 2022 18:05:02.834335089 CEST	587	49775	66.29.159.53	192.168.2.5	220 Ready to start TLS

Statistics

Behavior



System Behavior

Analysis Process: DHL DELIVERY.exe PID: **6860**, Parent PID: **4500**

General

Target ID:	1
Start time:	18:04:32
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DHL DELIVERY.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL DELIVERY.exe"
Imagebase:	0xa60000

File size:	574976 bytes
MD5 hash:	56A08FD913BFC20FA0F15A4FB204BAC9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.473923703.000000000452C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.473923703.000000000452C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.472974687.00000000043AB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.472974687.00000000043AB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.472421072.00000000042F2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_UACBypassusingCMSTP, Description: Yara detected UAC Bypass using CMSTP, Source: 00000001.00000002.472421072.00000000042F2000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.473251720.0000000004423000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.473251720.0000000004423000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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	6E495705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E495705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E49CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3F03DE	ReadFile

Analysis Process: DHL DELIVERY.exe PID: **6984**, Parent PID: **6860**

General

Target ID:	3
Start time:	18:04:44
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\DHL DELIVERY.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL DELIVERY.exe
Imagebase:	0xa60000
File size:	574976 bytes
MD5 hash:	56A08FD913BFC20FA0F15A4FB204BAC9
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: 00000003.00000002.692251401.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.692251401.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.463670113.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.463670113.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.464161754.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.464161754.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.462833671.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.462833671.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.461699324.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.461699324.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.695721560.0000000003121000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.695721560.0000000003121000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E4BCF06	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	6E4BCF06	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	6E495705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E495705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E49CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3F03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3F03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E495705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E495705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C061B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C061B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C061B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C061B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C061B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c3d0bcad-59c3-41fa-89dd-89b9005799af	unknown	4096	success or wait	1	6C061B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C061B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C061B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C061B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C061B4F	ReadFile

Disassembly

No disassembly