

JOeSandbox Cloud BASIC



ID: 562449

Sample Name: DHL airwaybill #
6913321715.pdf.exe

Cookbook: default.jbs

Time: 22:07:20

Date: 28/01/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report DHL airwaybill # 6913321715.pdf.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Threatname: Telegram RAT	4
Threatname: Agenttesla	4
Yara Overview	4
Memory Dumps	5
Unpacked PEs	5
Sigma Overview	5
System Summary	5
Jbx Signature Overview	5
AV Detection	5
System Summary	5
Data Obfuscation	6
Hooking and other Techniques for Hiding and Protection	6
Malware Analysis System Evasion	6
HIPS / PFW / Operating System Protection Evasion	6
Stealing of Sensitive Information	6
Remote Access Functionality	6
Mitre Att&ck Matrix	6
Behavior Graph	7
Screenshots	7
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	8
Initial Sample	8
Dropped Files	8
Unpacked PE Files	8
Domains	9
URLs	9
Domains and IPs	9
Contacted Domains	9
URLs from Memory and Binaries	9
World Map of Contacted IPs	11
General Information	11
Warnings	12
Simulations	12
Behavior and APIs	12
Joe Sandbox View / Context	13
IPs	13
Domains	13
ASNs	13
JA3 Fingerprints	13
Dropped Files	13
Created / dropped Files	13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL airwaybill # 6913321715.pdf.exe.log	13
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kmk.exe.log	13
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hwo33s0z.w1.psm1	14
C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ju3khw10.efd.ps1	14
C:\Users\user\AppData\Roaming\kmk\kmk.exe	15
C:\Users\user\AppData\Roaming\kmk\kmk.exe:Zone.Identifier	15
C:\Users\user\Documents\20220128\PowerShell_transcript.971342.ci0oIV5C.20220128220837.txt	15
Static File Info	16
General	16
File Icon	16
Static PE Info	16
General	16
Entrypoint Preview	16
Data Directories	18
Sections	18
Resources	19
Imports	19
Version Infos	19
Network Behavior	19
Statistics	19
Behavior	19
System Behavior	20
Analysis Process: DHL airwaybill # 6913321715.pdf.exePID: 6960, Parent PID: 2172	20

General	20
File Activities	20
File Created	20
File Written	20
File Read	21
Analysis Process: powershell.exePID: 6892, Parent PID: 6960	21
General	21
File Activities	22
File Created	22
File Deleted	22
File Written	22
File Read	24
Analysis Process: conhost.exePID: 6704, Parent PID: 6892	28
General	28
Analysis Process: DHL airwaybill # 6913321715.pdf.exePID: 6324, Parent PID: 6960	28
General	28
File Activities	29
File Created	29
File Written	29
File Read	30
Registry Activities	30
Key Value Created	30
Analysis Process: kmk.exePID: 7020, Parent PID: 3352	30
General	31
File Activities	31
File Created	31
File Written	31
File Read	32
Analysis Process: kmk.exePID: 5860, Parent PID: 7020	32
General	32
File Activities	33
File Created	33
File Read	33
Analysis Process: kmk.exePID: 4068, Parent PID: 3352	33
General	33
Disassembly	34

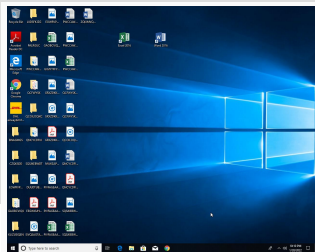
Windows Analysis Report

DHL airwaybill # 6913321715.pdf.exe

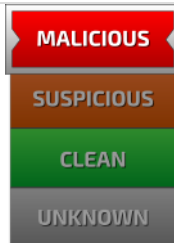
Overview

General Information

Sample Name:	DHL airwaybill # 6913321715.pdf.exe
Analysis ID:	562449
MD5:	3b20635ff80f8db..
SHA1:	cb5c019fe00f01b..
SHA256:	83ea16c53988fd..
Tags:	DHL exe
Infos:	       



Detection



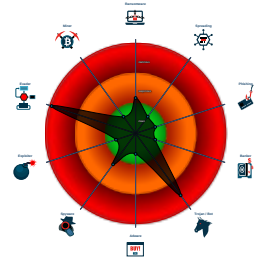
AgentTesla

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

Signatures

- | |
|---|
| Found malware configuration |
| Sigma detected: Suspicious Double... |
| Malicious sample detected (through... |
| Yara detected Telegram RAT |
| Yara detected AgentTesla |
| Yara detected AntiVM3 |
| Initial sample is a PE file and has a... |
| Tries to detect sandboxes and other... |
| Machine Learning detection for sam... |
| .NET source code contains potentia... |
| Injects a PE file into a foreign proce... |
| Sigma detected: Powershell Defend... |

Classification



Process Tree

Malware Configuration

Threatname: Telegram RAT

```
{
  "C2 url": "https://api.telegram.org/bot1952154144:AAEHUKomldKQIyjqg_Mhw4YwIGcA_iwz6T4/sendMessage"
}
```

Threatname: Agenttesla

```
{
  "Exfil Mode": "Telegram",
  "Chat id": "-561346972",
  "Chat URL": "https://api.telegram.org/bot1952154144:AAEHUKomldKQIyJgg_Mhw4YWiGcA_iwz6T4/sendDocument"
}
```

Yara Overview

Memory Dumps				
Source	Rule	Description	Author	Strings
00000017.00000000.430122857.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000000.430122857.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000017.00000000.427990557.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000000.427990557.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000E.00000000.336935642.0000000000402000.0000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 46 entries				

Unpacked PEs				
Source	Rule	Description	Author	Strings
23.0.kmk.exe.400000.6.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
23.0.kmk.exe.400000.6.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
23.0.kmk.exe.400000.6.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	0x30417:\$s1: get_kbok 0x30d4b:\$s2: get_CHoo 0x319a6:\$s3: set_passwordIsSet 0x3021b:\$s4: get_enableLog 0x3493b:\$s8: torbrowser 0x3331e:\$s10: logins 0x32bec:\$s11: credential 0x2f60a:\$g1: get_Clipboard 0x2f618:\$g2: get_Keyboard 0x2f625:\$g3: get_Password 0x30bf9:\$g4: get_CtrlKeyDown 0x30c09:\$g5: get_ShiftKeyDown 0x30c1a:\$g6: get_AltKeyDown
14.2.DHL airwaybill # 6913321715.pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
14.2.DHL airwaybill # 6913321715.pdf.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
Click to see the 63 entries				

Sigma Overview

System Summary



Sigma detected: Suspicious Double Extension
Sigma detected: Powershell Defender Exclusion

Jbx Signature Overview

AV Detection



Found malware configuration
Machine Learning detection for sample
Machine Learning detection for dropped file

System Summary



Malicious sample detected (through community Yara rule)
Initial sample is a PE file and has a suspicious name
.NET source code contains very large array initializations

Data Obfuscation



.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion



Yara detected AntiVM3

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

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

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

HIPS / PFW / Operating System Protection Evasion



Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information



Yara detected Telegram RAT

Yara detected AgentTesla

Remote Access Functionality

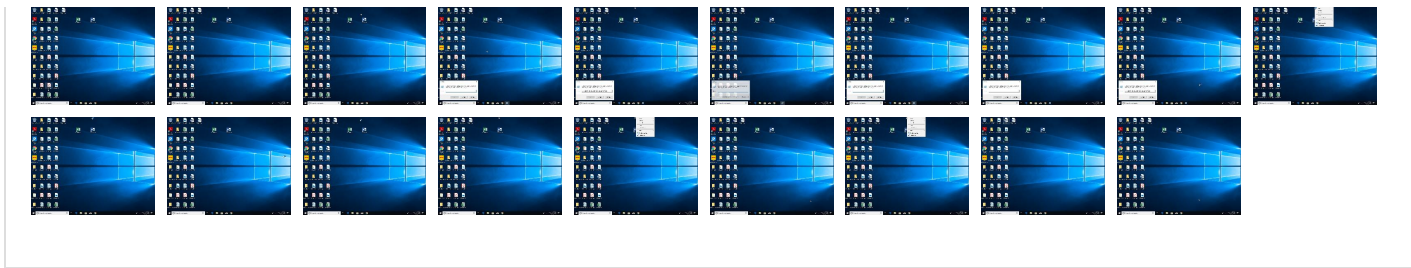


Yara detected Telegram RAT

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	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 1 Masquerading	OS Credential Dumping	1 Query Registry	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 1 Disable or Modify Tools	LSASS Memory	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 3 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	1 3 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
DHL airwaybill # 6913321715.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\kmk\kmk.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
23.0.kmk.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.2.DHL airwaybill # 6913321715.pdf.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Source	Detection	Scanner	Label	Link	Download
14.0.DHL airwaybill # 6913321715.pdf.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.2.kmk.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.kmk.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.kmk.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.kmk.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.DHL airwaybill # 6913321715.pdf.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
23.0.kmk.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.DHL airwaybill # 6913321715.pdf.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.DHL airwaybill # 6913321715.pdf.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
14.0.DHL airwaybill # 6913321715.pdf.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains
 No Antivirus matches

URLS				
Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://blog.iandreev.com/	0%	Virustotal		Browse
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://qDvGtL.com	0%	Avira URL Cloud	safe	
http://blog.iandreev.com	0%	Virustotal		Browse
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://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	

Domains and IPs
Contacted Domains
 No contacted domains info

URLs from Memory and Binaries				
Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	DHL airwaybill # 6913321715.pdf.exe, 0000000E.00000002.555730797.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000017.00000002.555059096.0000000002981000.00000004.00000800.00020000.000000.sdmp	false	Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://DynDns.comDynDNS	kmk.exe, 00000017.00000002.555059096.000000002981000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://blog.iandreev.com/	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.341357442.00000000027F1000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000014.00000002.437628452.00000000033A1000.00000004.00000800.00020000.0000000.sdmp, kmk.exe, 00000019.00000002.446345901.000000003041000.00000004.00000800.00020000.00000000.sdmp	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/?	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot1952154144:AAEHUKomldKQlyjgq_MWw4YWiGcA_iwz6T4/	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.344439121.00000000037F9000.00000004.00000800.00020000.00000000.sdmp, DHL airwaybill # 6913321715.pdf.exe, 0000000E.00000000.336935642.0000000000402000.00000040.00000400.00020000.00000000.sdmp, kmk.exe, 00000014.00000002.439979676.00000000043A9000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000017.00000000.430122857.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	DHL airwaybill # 6913321715.pdf.exe, 0000000E.0000002.555730797.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000017.00000002.555059096.0000000002981000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://qDvGtL.com	kmk.exe, 00000017.00000002.555059096.000000002981000.00000004.00000800.00020000.00000000.sdmp	false	Avira URL Cloud: safe	unknown
http://blog.iandreev.com	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.341357442.00000000027F1000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000014.00000002.437628452.00000000033A1000.00000004.00000800.00020000.0000000.sdmp, kmk.exe, 00000019.00000002.446345901.000000003041000.00000004.00000800.00020000.00000000.sdmp	false	0%, Virustotal, Browse - Avira URL Cloud: safe	unknown
http://www.tiro.com	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.carterandcone.coml	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://api.telegram.org/bot1952154144:AAEHUKomldKQlyjgq_MWw4YWiGcA_iwz6T4/sendDocumentdocument----	DHL airwaybill # 6913321715.pdf.exe, 0000000E.0000002.555730797.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000017.00000002.555059096.0000000002981000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sajatypeworks.com	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.typography.netD	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://fontfabrik.com	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.founder.com.cn/cn	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.urwpp.deDPlease	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nam e	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.341357442.00000000027F1000.00000004.00000800.00020000.00000000.sdmp, DHL airwaybill # 6913321715.pdf.exe, 00000000.00000002.342180539.00000000028A9000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000014.00000002.437628452.00000000033A1000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000014.00000002.438006556.000000000346D000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.346542167.0000000006982000.00000004.00000800.00020000.00000000.sdmp	false	URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	DHL airwaybill # 6913321715.pdf.exe, 00000000.0000002.344439121.00000000037F9000.00000004.00000800.00020000.00000000.sdmp, DHL airwaybill # 6913321715.pdf.exe, 0000000E.00000000.336935642.000000000402000.00000040.00000400.00020000.00000000.sdmp, kmk.exe, 00000014.00000002.439979676.00000000043A9000.00000004.00000800.00020000.00000000.sdmp, kmk.exe, 00000017.00000000.430122857.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562449
Start date:	28.01.2022
Start time:	22:07:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL airwaybill # 6913321715.pdf.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:	29
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.evad.winEXE@10/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.9%) • Quality average: 55.5% • Quality standard deviation: 33.1%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, ctdl.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 creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have 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
22:08:34	API Interceptor	610x Sleep call for process: DHL airwaybill # 6913321715.pdf.exe modified
22:08:39	API Interceptor	39x Sleep call for process: powershell.exe modified
22:09:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run kmk C:\Users\user\AppData\Roaming\kmk\kmk.exe
22:09:13	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run kmk C:\Users\user\AppData\Roaming\kmk\kmk.exe
22:09:18	API Interceptor	273x Sleep call for process: kmk.exe modified

SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
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\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\1b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	20524
Entropy (8bit):	5.577004178466104
Encrypted:	false
SSDEEP:	384:itADL0qVRhEq0hakMSBK n9jultVP7Y9gtSJ3xeT1MaXZIXzFCldd:ZeqAc4K9CltSrc8C+fjS
MD5:	575E183C46DF2B94849B3A83A75F4B79
SHA1:	D96BD087C175AAE17CD6FFB9DD1A82EEBDEEC1B3
SHA-256:	EC988F6C702825E1B71A91127AF96AE625A950C6CDC6A1461FBE197BB434F1B2
SHA-512:	8142D869987C259E832F2217A2A14975BEE403AB70A26BC6351265C67E15DD0CC91B484F3B78FF5FA1DF29446CD3E51BDE5FA42099A84D160AFE5EC3D7602AE0
Malicious:	false
Reputation:	low
Preview:	@...e.....h.....n...G.....@.....H.....<@^L."My..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F....x.)\.....System.Management.Automation4.....[...[a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5...O.g..q.....System.Xml.L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'.....L..}).....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management..4.....].D.E...#.....System.Data.H..... ..H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...\$.1.q.....System.ConfigurationP...../C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-D.F.<.;nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_hwo33s0z.w1L.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp_PSScriptPolicyTest_ju3khw10.efd.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B

SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\kmk\kmk.exe 	
Process:	C:\Users\user\Desktop\DHL airwaybill # 6913321715.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	858624
Entropy (8bit):	6.554532266693901
Encrypted:	false
SSDEEP:	12288:1Jo9T57wb74Ab5327wrXE9iMUfe3mWLZ:vo37wP4AbJ/XEYMUW3ma
MD5:	3B20635FF80F8DB4517F4BF9E2E79277
SHA1:	CB5C019FE00F01B08EBB33247E0093C761291F3C
SHA-256:	83EA16C53988FD7E522FA373EE71089AC84CDFBD8CDEA6C5A54AFC61A5FC0389
SHA-512:	326F3AE24C61A304648EC1720BE33090C9DF648CF34D183C113EAE1CF8FED35891CE3A4F80DBBF3990591B0F0A6553A696A6E849345C0F6D344E513F2BE45231
Malicious:	true
Antivirus:	Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....PE..L...+..a.....!... ..@...@..@..... ..K...`..... ..H.....text..4... ..`..sdata.....@.....@...rsrc.....`@...@...reloc.....@...B.....

C:\Users\user\AppData\Roaming\kmk\kmk.exe:Zone.Identifier 	
Process:	C:\Users\user\Desktop\DHL airwaybill # 6913321715.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	true
Preview:	[ZoneTransfer].....ZoneId=0

C:\Users\user\Documents\20220128\PowerShell_transcript.971342.ci0oIV5C.20220128220837.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3559
Entropy (8bit):	5.351882714564832
Encrypted:	false
SSDEEP:	96:BZOhQNcvqDo1Z523LLZ4hQNcvqDo1Zpq3L53Lkv30c3Lkv30c3Lkv30mTZMq:cHiAy1kv3Hkv3Hkv37qq
MD5:	7F650C889B17D2475F4241004CB3F237
SHA1:	A85EA0A1EB712602E0EBB762BC20B4FB5EA8BE5D
SHA-256:	221DCAA70A34E73462EA2915B4F0BF45141A49D91ADABFDB81BA0C84FD10C7A1
SHA-512:	F8724F646B3A3A3EED8CCD93ACBC8E76C1AF2DD7FE61EB98A0DA25B1FD27C3E24168634EA40199E99D179889B99DA1347E7450A0C2551275B023878F34BF74E
Malicious:	false
Preview:	.*****.Windows PowerShell transcript start..Start time: 20220128220838..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 971342 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference - ExclusionPath C:\Users\user\Desktop\DHL airwaybill # 6913321715.pdf.exe..Process ID: 6892..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..Serializati onVersion: 1.1.0.1..***** ..*****..Command start time: 20220128220838..***** ..PS>Add-MpPreference -ExclusionPath C:\User s\user\Desktop\DHL airwaybill # 6913321715.pdf.exe..***** ..Command start time: 20220128221204..***** ..PS>TerminatingError(Add- MpPreference): "A po



[illegible]

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd20e0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd6000	0xf0c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd8000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd208e	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
.text	0x2000	0xd0134	0xd0200	False	0.514625563063	data	6.56605144974	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.sdata	0xd4000	0x1e8	0x200	False	0.861328125	data	6.61461864943	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xd6000	0xf0c	0x1000	False	0.3388671875	data	3.41623205457	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

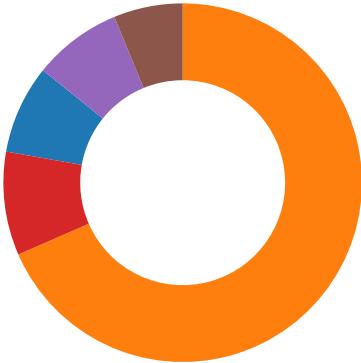
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xd8000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
RT_ICON	0xd6130	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 0, next used block 0		
RT_GROUP_ICON	0xd69d8	0x14	data		
RT_VERSION	0xd69ec	0x334	data		
RT_MANIFEST	0xd6d20	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 2016
Assembly Version	1.0.0.0
InternalName	ExceptionArgume.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	OthelloCS
ProductVersion	1.0.0.0
FileDescription	OthelloCS
OriginalFilename	ExceptionArgume.exe

Network Behavior
 No network behavior found

Statistics
Behavior
 - DHL airwaybill # 6913321715.pdf.ex... - powershell.exe - conhost.exe - DHL airwaybill # 6913321715.pdf.ex... - kmk.exe - kmk.exe - kmk.exe

System Behavior

Analysis Process: DHL airwaybill # 6913321715.pdf.exe PID: 6960, Parent PID: 2172

General

Target ID:	0
Start time:	22:08:12
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\DHL airwaybill # 6913321715.pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\DHL airwaybill # 6913321715.pdf.exe"
Imagebase:	0x4b0000
File size:	858624 bytes
MD5 hash:	3B20635FF80F8DB4517F4BF9E2E79277
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: 00000000.00000002.341357442.00000000027F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.342180539.00000000028A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.344439121.00000000037F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.344439121.00000000037F9000.00000004.00000800.00020000.00000000.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	6E77CF06	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	6E77CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL airwaybill # 6913321715.pdf.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6EA8C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL airwaybill # 6913321715.pdf.exe.log	0	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6EA8C907	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	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E755705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\la152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E75CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D5C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile	

Analysis Process: powershell.exe PID: 6892, Parent PID: 6960	
General	
Target ID:	12
Start time:	22:08:35
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\DHL airwaybill # 6913321715.pdf.exe
Imagebase:	0xfe0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

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	6E77CF06	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	6E77CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_ju3khw0.efd.ps1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6D5C1E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_hwo33s0z.w1l.psm1	read attributes synchronize generic write	device	sequential only synchronous io non alert non directory file open no recall	success or wait	1	6D5C1E60	CreateFileW
C:\Users\user\Documents\20220128	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D5CBEFF	CreateDirectoryW
C:\Users\user\Documents\20220128\PowerShell_transcript.971342.ci0oIV5C.20220128220837.txt	read attributes synchronize generic read generic write	device	synchronous io non alert non directory file open no recall	success or wait	1	6D5C1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_ju3khw0.efd.ps1	success or wait	1	6D5C6A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hwo33s0z.w1l.psm1	success or wait	1	6D5C6A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_ju3khw0.efd.ps1	0	1	31	1	success or wait	1	6D5C1B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscripPolicyTest_hwo33s0z.w1l.psm1	0	1	31	1	success or wait	1	6D5C1B4F	WriteFile
C:\Users\user\Documents\20220128\PowerShell_transcript.971342.ci0oIV5C.20220128220837.txt	0	3	ff		success or wait	1	6D5C1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	1088	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 00 01 24 4d 00 01 16 3b 40 01 38 4d 00 01 3f 4d 00 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40 01 57 03 40 01 4d 03 40 01 fd 45 40 01 42 4d 00 01 fd 44 00 01 6d 45 00	T@>@@V@H@X@[@N T@HT@S@S@hT@S@ S@S@\\T@T@X@? X@T@S@S@T@T@xT @zT@ T@=M@DM@:M@"M@ M@!M@;M@D@D@@M @<M\$M;@8M? M;@;@<@<@W@M @E@BMDmE	success or wait	10	6EA476FC	WriteFile

File Read							
File Path	Offset	Length	Completion	Count	Source Address	Symbol	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E755705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E755705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\1a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E75CA54	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E75CA54	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E75CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E755705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E755705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E755705	unknown	
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E755705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E755705	unknown	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	unknown	64	success or wait	1	6E761F73	ReadFile	
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StarterProfileData-NonInteractive	unknown	23200	success or wait	1	6E76203F	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E6B03DE	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6D5C1B4F	ReadFile	
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile	

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	5	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	131	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6D5C1B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E6B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E6B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E6B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E6B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E6B03DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E755705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E755705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	3	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E755705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E755705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	4096	success or wait	3	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\len-US\BitLocker.psd1	unknown	770	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	68	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	12	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6D5C1B4F	ReadFile
C:\Windows\Microsoft.NET\Assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6E73D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6E73D72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D5C1B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D5C1B4F	ReadFile

Analysis Process: conhost.exe PID: 6704, Parent PID: 6892

General

Target ID:	13
Start time:	22:08:36
Start date:	28/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: DHL airwaybill # 6913321715.pdf.exe PID: 6324, Parent PID: 6960

General

Target ID:	14
Start time:	22:08:36
Start date:	28/01/2022
Path:	C:\Users\user\Desktop\DHL airwaybill # 6913321715.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL airwaybill # 6913321715.pdf.exe
Imagebase:	0xb20000
File size:	858624 bytes
MD5 hash:	3B20635FF80F8DB4517F4BF9E2E79277
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: 0000000E.00000000.336935642.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.336935642.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.335084179.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.335084179.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.556837091.0000000003044000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.336274774.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.336274774.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000000.335645947.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000000.335645947.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.549151851.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.549151851.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.555730797.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 0000000E.00000002.555730797.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.555730797.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 0000000E.00000002.555730797.0000000002F91000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen
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	6E77CF06	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	6E77CF06	unknown	
C:\Users\user\AppData\Roaming\kmk	read data or list directory synchronize	device	directory file synchronous io non alert open for backup ident open reparse point	success or wait	1	6D5CBEFF	CreateDirectoryW	
C:\Users\user\AppData\Roaming\kmk\kmk.exe	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	6D5CDD66	CopyFileW	
C:\Users\user\AppData\Roaming\kmk\kmk.exe\Zone.Identifier:\$DATA	read data or list directory synchronize generic write	device	sequential only synchronous io non alert	success or wait	1	6D5CDD66	CopyFileW	

File Path					Completion	Count	Source Address	Symbol
File Written								
File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

General	
Target ID:	20
Start time:	22:09:13
Start date:	28/01/2022
Path:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kmk\kmk.exe"
Imagebase:	0xf70000
File size:	858624 bytes
MD5 hash:	3B20635FF80F8DB4517F4BF9E2E79277
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	- Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.439979676.00000000043A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.439979676.00000000043A9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.437628452.00000000033A1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security - Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.43806556.000000000346D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	Detection: 100%, Joe Sandbox ML
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	6E77CF06	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	6E77CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kmk.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6EA8C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
-----------	--------	--------	-------	-------	------------	-------	----------------	--------

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\kmk.exe.log	0	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",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6EA8C907	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	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E755705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae4ee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E75CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefaf3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D5C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile	

Analysis Process: kmk.exe PID: 5860, Parent PID: 7020	
General	
Target ID:	23
Start time:	22:09:19
Start date:	28/01/2022
Path:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
Imagebase:	0x450000
File size:	858624 bytes
MD5 hash:	3B20635FF80F8DB4517F4BF9E2E79277
Has elevated privileges:	false

Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.430122857.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.430122857.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.427990557.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.427990557.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.549128937.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.549128937.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.555059096.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000017.00000002.555059096.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000017.00000002.555059096.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000017.00000002.555059096.0000000002981000.00000004.00000800.00020000.00000000.sdmp, Author: ditekShen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.428617540.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.428617540.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000000.427541132.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000000.427541132.0000000000402000.00000040.00000400.00020000.00000000.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	6E77CF06	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	6E77CF06	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	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E755705	unknown	
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77ae03305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E75CA54	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E6B03DE	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E755705	unknown	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D5C1B4F	ReadFile	
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D5C1B4F	ReadFile	

Analysis Process: kmk.exe PID: 4068, Parent PID: 3352

General

Target ID:	25
Start time:	22:09:21
Start date:	28/01/2022
Path:	C:\Users\user\AppData\Roaming\kmk\kmk.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\kmk\kmk.exe"
Imagebase:	0xbf0000
File size:	858624 bytes
MD5 hash:	3B20635FF80F8DB4517F4BF9E2E79277
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Reputation:	low

Disassembly

 No disassembly