ID: 800700
Sample Name: DHL AWB SHIPPING DOCS_AWB_0009123.exe
Cookbook: default.jbs
Time: 18:23:13
Date: 07/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

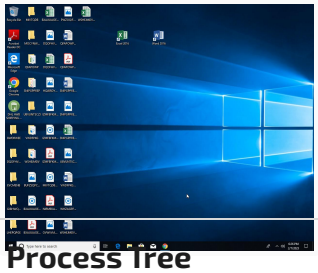
Windows Analysis Report

DHL AWB SHIPPING DOCS_AWB_0009123.exe

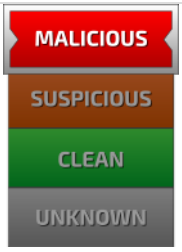
Overview

General Information

Sample Name:	DHL AWB SHIPPING DOCS_AWB_0009123.exe
Analysis ID:	800700
MD5:	cf98f42b9d4bb…
SHA1:	254308038623…
SHA256:	f7b57c7265e87..
Tags:	DHL exe SnakeKeylogger
Infos:	



Detection



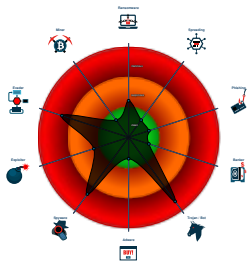
Snake Keylogger

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

Signatures

- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Multi AV Scanner detection for drop…
- Snort IDS alert for network traffic
- Tries to steal Mail credentials (via fi…
- Maps a DLL or memory area into an…
- Tries to harvest and steal ftp login c…
- .NET source code references suspic…
- May check the online IP address of…
- Found evasive API chain (may stop…

Classification



Process Tree

- **System is w10x64**
- DHL AWB SHIPPING DOCS_AWB_0009123.exe (PID: 1772 cmdline: C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe MD5: CF98F42B9D4BBDC20E54E7E0CA7543C0)
  - tdbwdaltxz.exe (PID: 5884 cmdline: "C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe" C:\Users\user\AppData\Local\Temp\rjnyysvx.m MD5: 377552A9A2C84B8C55314176A566C079)
    - tdbwdaltxz.exe (PID: 5864 cmdline: C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe MD5: 377552A9A2C84B8C55314176A566C079)
    - MpCmdRun.exe (PID: 2576 cmdline: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable MD5: A267555174BFA53844371226F482B86B)
      - conhost.exe (PID: 6048 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "Telegram",
  "Telegram URL": "https://api.telegram.org/bot6155153237:AAHwniNOLh5IeMqe3WWu52NIjrXAphPX4U4/sendMessage?chat_id=5463149861"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth (Nextron Systems)	• 0x2ecb8:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x2deea:$a3: \Google\Chrome\User Data\Default\Login Data • 0x2e31d:$a4: \Orbitum\User Data\Default\Login Data • 0x2f444:$a5: \Kometa\User Data\Default\Login Data

Source	Rule	Description	Author	Strings
00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp	INDICATOR_SUSPICIOUS_EXE_DotNetProcHook	Detects executables with potential process hoocking	ditekSHen	• 0x28192:$s1: UnHook • 0x28199:$s2: SetHook • 0x281a1:$s3: CallNextHook • 0x281ae:$s4: _hook
Click to see the 42 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.tdbwdaltxz.exe.3c15530.6.raw.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth (Nextron Systems)	• 0x1b660:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x1a892:$a3: \Google\Chrome\User Data\Default\Login Data • 0x1acc5:$a4: \Orbitum\User Data\Default\Login Data • 0x1bdec:$a5: \Kometa\User Data\Default\Login Data
2.2.tdbwdaltxz.exe.3c15530.6.raw.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
2.2.tdbwdaltxz.exe.3c15530.6.raw.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
2.2.tdbwdaltxz.exe.3c15530.6.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
2.2.tdbwdaltxz.exe.3c15530.6.raw.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 106 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.2.3 - Destination IP: 193.122.6.168

Timestamp:	192.168.2.3193.122.6.16849700802039190 02/07/23-18:24:17.350492
SID:	2039190
Source Port:	49700
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking

Snort IDS alert for network traffic

May check the online IP address of the machine

Yara detected Generic Downloader

System Summary

Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

.NET source code references suspicious native API functions

Stealing of Sensitive Information

Yara detected Snake Keylogger

Yara detected Telegram RAT

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

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

Yara detected Snake Keylogger

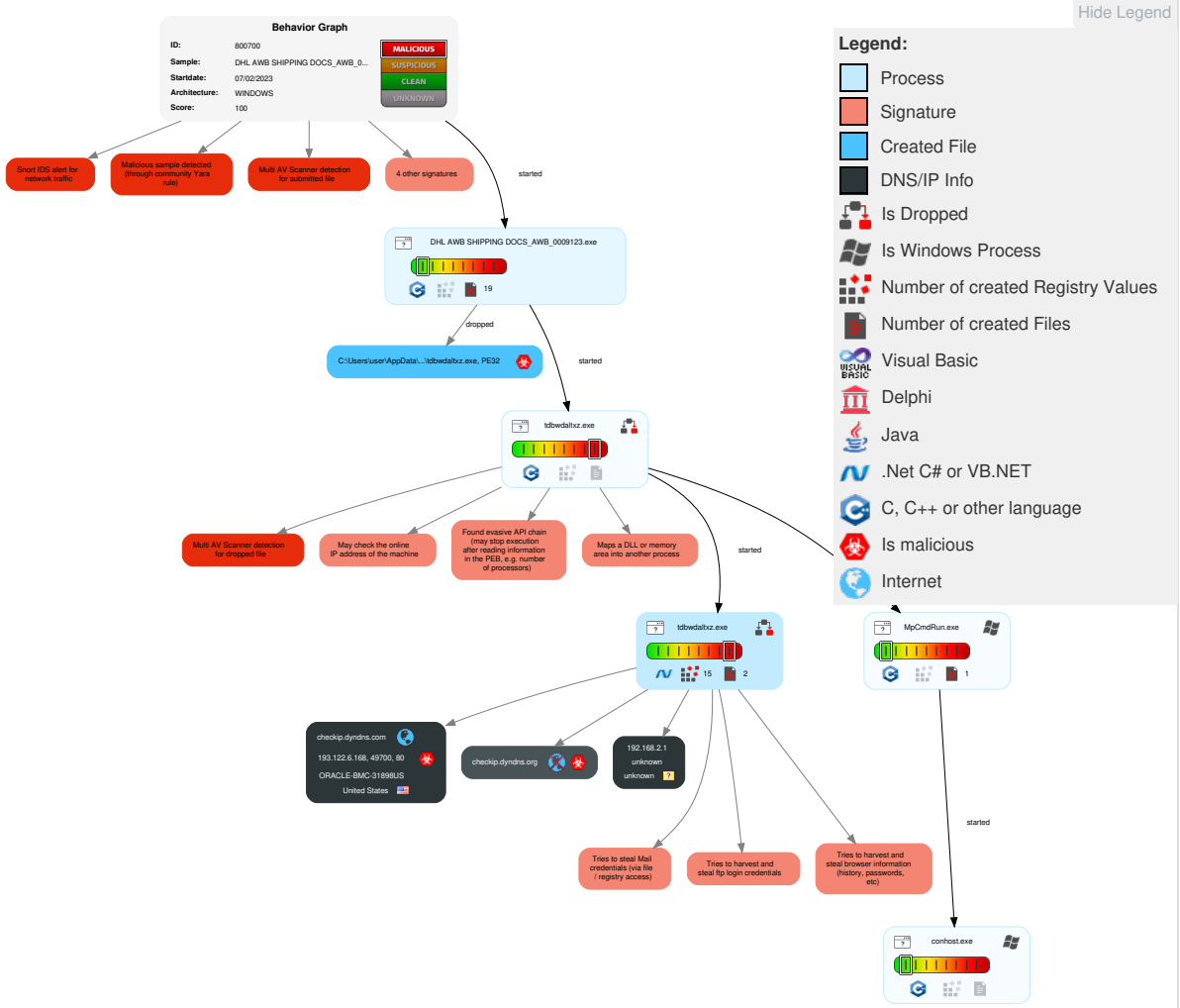
Yara detected Telegram RAT

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	1 Windows Management Instrumentation	1 1 Windows Service	1 Access Token Manipulation	1 Disable or Modify Tools	2 OS Credential Dumping	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	2 1 Native API	Boot or Logon Initialization Scripts	1 1 Windows Service	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	3 Command and Scripting Interpreter	Logon Script (Windows)	1 1 1 Process Injection	3 1 Obfuscated Files or Information	Security Account Manager	3 7 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	2 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Service Execution	Logon Script (Mac)	Logon Script (Mac)	1 Software Packing	NTDS	1 4 1 Security Software Discovery	Distributed Component Object Model	1 Clipboard Data	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Access Token Manipulation	LSA Secrets	1 Process 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	1 1 1 Process Injection	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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

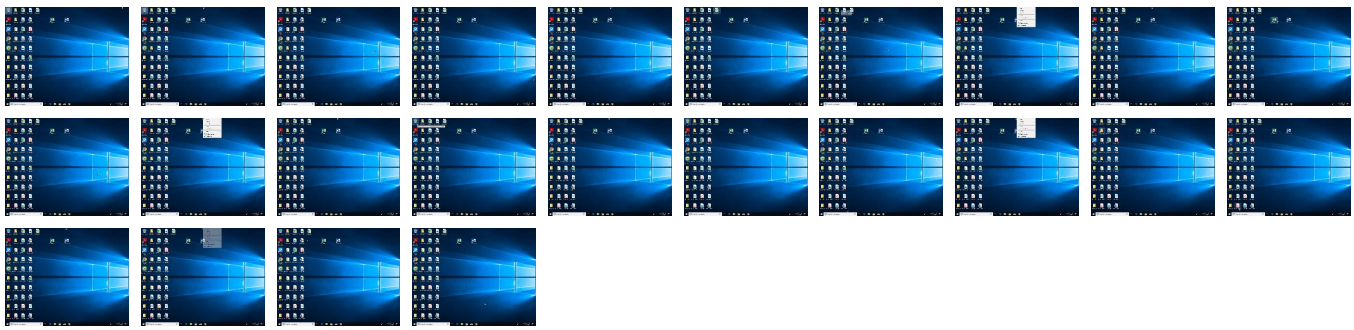
Behavior Graph



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 AWB SHIPPING DOCS_AWB_0009123.exe	44%	ReversingLabs	Win32.Trojan.Nsisx	
DHL AWB SHIPPING DOCS_AWB_0009123.exe	37%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe	23%	ReversingLabs	Win32.Trojan.InjectorX	
C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe	13%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.tdbwdaltxz.exe.400000.1.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
2.2.tdbwdaltxz.exe.2b40000.5.unpack	100%	Avira	HEUR/AGEN.1203035		Download File

Domains

Source	Detection	Scanner	Label	Link
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://checkip.dyndns.org4	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://schemas.m	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	URL Reputation	safe	
http://checkip.dyndns.com	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checkip.dyndns.com	193.122.6.168	true	true	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

Contacted URLs

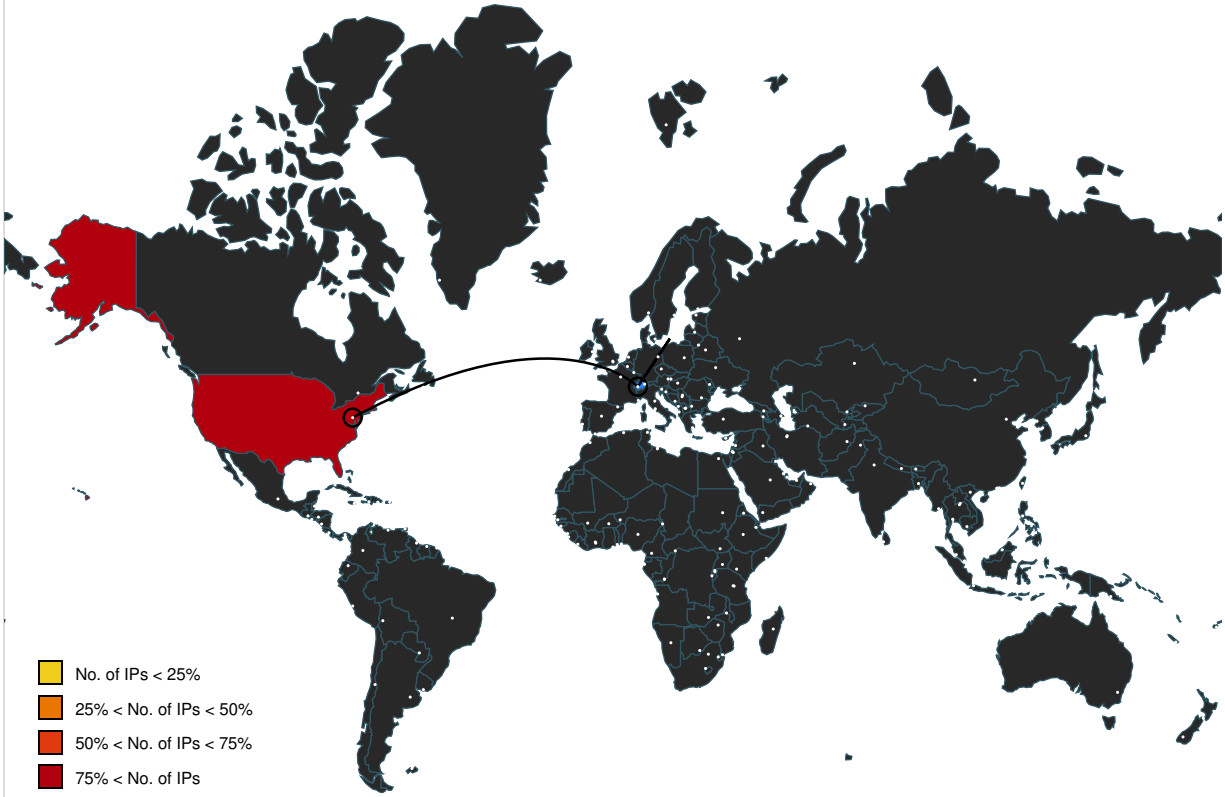
Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org4	tdbwdaltxz.exe, 00000002.00000002.519971304.0000000002CA7000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org	tdbwdaltxz.exe, 00000002.00000002.519971304.0000000002CA7000.00000004.00000800.00020000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.519971304.0000000002CB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.m	tdbwdaltxz.exe	false	• URL Reputation: safe	unknown
http://checkip.dyndns.com	tdbwdaltxz.exe, 00000002.00000002.519971304.0000000002CB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	DHL AWB SHIPPING DOCS_AWB_0009123.exe	false		high
http://https://api.telegram.org/bot	tdbwdaltxz.exe, tdbwdaltxz.exe, 00000002.00000002.520282991.0000000003C11000.00000004.00000800.00020000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.519032371.0000000000EE9000.00000004.00000020.00020000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.519618240.0000000002B42000.00000040.00001000.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	tdbwdaltxz.exe, 00000002.00000002.519971304.0000000002C11000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/q	tdbwdaltxz.exe, 00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.520282991.0000000003C11000.00000004.00000800.00020000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.519032371.0000000000EE9000.00000004.00000020.00020000.00000000.sdmp, tdbwdaltxz.exe, 00000002.00000002.519618240.0000000002B42000.00000040.00001000.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
193.122.6.168	checkip.dyndns.com	United States		31898	ORACLE-BMC-31898US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	800700
Start date and time:	2023-02-07 18:23:13 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211

Number of analysed new started processes analysed:	14
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
Sample file name:	DHL AWB SHIPPING DOCS_AWB_0009123.exe
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@7/5@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24% (good quality ratio 22.1%) • Quality average: 81.2% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): SgrmBroker.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, ctldl.windowsupdate.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 getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:25:30	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\nsq9965.tmp

Process:	C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe
File Type:	data
Category:	dropped
Size (bytes):	384998
Entropy (8bit):	7.53345051811731
Encrypted:	false
SSDEEP:	6144:GiNgXKy76cANX89+opVo/l5YuNWfD4uFKjUP8dIZpSuAL+/zVM4/aN8OCTGdc+Vo:GiN1IcANX8kopVo/l5YuNiD4djBdM3Am
MD5:	C2CBFC18756BC145C8A0907ED158105A
SHA1:	87E0D94172166CBD10BF258BA60062662A073F96
SHA-256:	3D567DCC795B1B3BF6E755BBA0ADF2FB9C771039CFCA9BC8B1C9EFA0D4C5059C
SHA-512:	4ACEAD4873FCAFA93C771CB969D4CD315C32B6374F2FA4B03DB45606DF3F714C421E668421A6D5ACBE0BB9605DF9FE13F6193EA99FB46C8935E5756E9206E1FD
Malicious:	false
Reputation:	low
Preview:	.9.....,.....(.....8.....j9.....%..... .....G.....j.....p.....F..... ....

C:\Users\user\AppData\Local\Temp\rjnyysvx.m

Process:	C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe
File Type:	data
Category:	dropped
Size (bytes):	5952
Entropy (8bit):	7.144643695336174
Encrypted:	false
SSDEEP:	96:Farc6oYTg/DrYu0bk2XO5oSw0Qj7KPZ4dNriFdndNiPKqWuAbS4Vuw1OlH1l9I:FarcRXYhX1SJSKPZQRinndcZ2bS4Vuw7
MD5:	6C5E26AD7985FBE1F56D400664E1F130
SHA1:	6719DF376987B06E9D5410931F3341D0F34CBF14
SHA-256:	28240426EE93AFD8466A587C3E1985F410136B71CA176C7AF36CF0E01153C32D
SHA-512:	484BDF3D8FAC11086184A3300BEFAF4E7EC19C6CBD82FD15387BB2FC2240B7D2770767A0953D77A799069E096A89039AEDD35DE6C85F1A44CEF00AE062C5744
Malicious:	false
Reputation:	low
Preview:	.005m..f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c. .....4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4.....F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e...548.r...t..w.(058. q..v..l.0A..q..34.q.p.}..u.{.w....}.p013.....u.L.4F".u..04.t.t.q..p.x.u....q.8580..Y...}..E.4D'.q..80.}.t.t..w.p.p...X+AK..M.....v.ZXK.J.E.....}.]..O.F.....u.X_.M.M.....H...X...K.D.....}. \&....A..B....G...P5..O.E..P....\...Y...K.E..a....B...].4.T.4.q0.p..q..~<1|..x.q.>.t&.u.|1,.t..w.pe..\...w.p..u.T.4.Q.0.}.:.;q%..5M%.}.;.qm..tL9.}.5013.6.].5.u...K...P3480..u...dR0. m...D4...B358.q.0342.}.e.....dX4R0]<048[3^2^8Z5..p...d.a..

C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe

Process:	C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	133120
Entropy (8bit):	6.4113662500317306
Encrypted:	false
SSDEEP:	1536:idx1IKgbTK9n+iO2UzWe1+M+v6TGabh/b9QWWGuld6YpcA2suPtMO/b6qf7meggO:g1+a614qVbh/b9QWpocYpxEtPf7megt
MD5:	377552A9A2C84B8C55314176A566C079
SHA1:	EEDD3BD9AE6661E41BD8CE989AEF58383AB5B360
SHA-256:	4ADA7E83E7FFA97F90588475D5C9356A9F1003E1CC7721D227CA0609EF23E9DC
SHA-512:	554D8AAEBBB117E12798F6B7CADA554A49F332F91912A44503709E6022387A06FD46DBFA47E5E0B855DD5331A451C4C502AA77589533671BEA894B1B62C7D385
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23% • Antivirus: Virustotal, Detection: 13%, Browse

Reputation:	low
Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$........?..D^.D^.D^..>._^..<.N^..?.)^.D^..^.)H.]^.c.?.E^.c.8.E^.c.=.E ^.RichD^.........PE..L......c...........................UD............@..........................`...........@................................|........0......................@..........................................@.................. ..........................text............................. ..`.rdata...D.......F.................@..@.data....-.........................@....rsrc........0......................@..@.reloc..L....@......................@..B...... ....

C:\Users\user\AppData\Local\Temp\wfpxt.ubj	
Process:	C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe
File Type:	data
Category:	dropped
Size (bytes):	231188
Entropy (8bit):	7.955184590739643
Encrypted:	false
SSDEEP:	6144:6iNgXKy76cANX89+opVo/l5YuNWfD4uFKjUP8dIZpSuAL+/zVM4/aN8OCX:6iN1lcANX8kopVo/l5YuNiD4djBdM3AS
MD5:	912FD2CFFA357488F81E8C626E176050
SHA1:	67ED3E87F65DC8DA0522AD5246BB9307A5C451E0
SHA-256:	EF39E2F328D3AF0F953FBE899102F6689A41F12D5160F005815D4F619D9BFD31
SHA-512:	602109846C9CA54898775F4E24761759FC9D87805B44301BFDABC5C6A4D4414A37414E9DDBDC0370CF642A717689A71EDFEBB6EB2DE664A2DE5819A6882706E
Malicious:	false
Reputation:	low
Preview:	.n+.....{.K.u.).4p.....].....a...u..{.n BW6.P..:....Y..U..P...../.?.<`A...7.!.o-^I,.....T.d..q...B.1.....P.B.#2....,....G.........5...p...G..By.Zf..<c5..P.....<....4t......Z.)KI!LxY)..780.zT..H.8i..}. ..8.*l.m(......a.7..fR:.pR.....<.R.|.>RM...E........K..s.........]....!F.xwL.%u..9n BW6R...:M....Y..e.*.p'..SE.......t..?.H..Nk..+...3.w....~.>.S.X.y.d9.%u.(f.....,...`.&=.q,.d...yh..:U.p.K1 ;.k.-.>K#.c.2hX.Ub.....2G.&Q....P....>W.R..,.u.d..D}\@...aL...R....'.y..U+.....O........zz<|.>RM...cP.0.....K.Q.).6)...I..].....a....u....E9DW6U...:.....Y.KU.*.p'..SE@..........F.. N.;e+...3.y.....>...X.y.d9.%|.(.N .@+,.....&=.+,...LC........K1;.kJ-.K#.c.2hX.Ub.......&3....P....>W.R..,.u.d..D}\@M...L...R....'.y..U......O........zz<|.>RM...E......d.K.Q.).6p......].....a ...u..{.n BW6.P..:....Y..U.*.p'..SE@......t..?.H..Nk[e+...3.w....~.>...X.y.d9.%u.(f.....,...`.&=.q,.@.Lyh........K1;.k.-.>K#.c.2hX.Ub.......&3....P....>W.R..,.u.d..D}\@M...L...R... .'.y..U....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	Unicode text, UTF-16, little-endian text, with CRLF line terminators
Category:	modified
Size (bytes):	10874
Entropy (8bit):	3.164510375794696
Encrypted:	false
SSDEEP:	192:cY+38+DJl+ibJ6+ioJJ+i3N+WtT+E9tD+Ett3d+E3z5+6I3+zJE+v:j+s+v+b+P+m+0+Q+q+q+73+zG+v
MD5:	689711D9AFE7F82E830AA6B2B8A2B83C
SHA1:	F6457E7D7B5120C6C80F9456412816CFB3F9B0E7
SHA-256:	A3D02EC8E3DF05FC4CBF1BD7B57E7DCDC051F6D50C71BC0B3B7E0EF42154962F
SHA-512:	B8D3DAC5FB3B2862C889B012F1BB740F9E6E4AB62E010070B0148E26276863D86C839C8CB0C29C85EBA87B8DDDFE10F8CBB21F0681754643430178C648D778D 2
Malicious:	false
Reputation:	low
Preview:	..........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. . L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0. 1.:.2.9.:.4.9.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. . (.8.0.0.7.0.4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. T.h.u. .. J.u.n. .. 2.7. .. 2.0.1.9. .0.1.:.2.9.:.4.9.....- .-............-.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.186130988184906
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	DHL AWB SHIPPING DOCS_AWB_0009123.exe
File size:	459101
MD5:	cf98f42b9d4bbdc20e54e7e0ca7543c0
SHA1:	2543080386230d110b18e1b653c14d1d640998da

SHA256:	f7b57c7265e87bee11e652eba90afe3e0c34f691cd8faf3b79fe8def96044831
SHA512:	2a84ede5f78203d417dd00af7f70e6bc2d50f5fc3859684a10be7e2448262b1e9334c6dfc064df7feb1b302d01b9b41ce8a9880473f246bf6af7cb601c9875f0
SSDEEP:	6144:sYa6RpFXx6QR4FUJE0S3u+vMwejAFbF6L5XamozD/DDX2zA:sYjpFXxJR40Ef3NMwekf6L5amozD3t
TLSH:	9AA4E68118CFC40DC35E3633A5E1C52A68D0CE326057632E771ABF8EB53BB4A5B4E659
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	e8f0e84c44e4e4f8

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	61259b55b8912888e90f516ca08dc514

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F336C80B17Ah

Instruction
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F336C80B14Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3b000	0x2a610	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.6568134014423077	data	6.4174599871908855	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.141066817170598	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.110582127654237	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.ndata	0x2b000	0x10000	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x3b000	0x2a610	0x2a800	False	0.15715188419117648	data	4.69978633667236	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3b358	0x10828	Device independent bitmap graphic, 128 x 256 x 32, image size 67584	English	United States
RT_ICON	0x4bb80	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 38016	English	United States
RT_ICON	0x55028	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 21600	English	United States
RT_ICON	0x5a4b0	0x4228	Device independent bitmap graphic, 64 x 128 x 32, image size 16896	English	United States
RT_ICON	0x5e6d8	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9600	English	United States
RT_ICON	0x60c80	0x225f	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced	English	United States
RT_ICON	0x62ee0	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4224	English	United States
RT_ICON	0x63f88	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 2400	English	United States
RT_ICON	0x64910	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 1088	English	United States
RT_DIALOG	0x64d78	0x100	data	English	United States
RT_DIALOG	0x64e78	0x11c	data	English	United States
RT_DIALOG	0x64f98	0x60	data	English	United States
RT_GROUP_ICON	0x64ff8	0x84	data	English	United States
RT_VERSION	0x65080	0x250	data	English	United States
RT_MANIFEST	0x652d0	0x33e	XML 1.0 document, ASCII text, with very long lines (830), with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

DLL	Import
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3193.122.6.168 49700802039190 02/07/23-18:24:17.350492	TCP	2039190	ET TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49700	80	192.168.2.3	193.122.6.168

Network Port Distribution

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:24:17.331041098 CET	49700	80	192.168.2.3	193.122.6.168
Feb 7, 2023 18:24:17.349941015 CET	80	49700	193.122.6.168	192.168.2.3
Feb 7, 2023 18:24:17.350086927 CET	49700	80	192.168.2.3	193.122.6.168
Feb 7, 2023 18:24:17.350492001 CET	49700	80	192.168.2.3	193.122.6.168
Feb 7, 2023 18:24:17.368350029 CET	80	49700	193.122.6.168	192.168.2.3
Feb 7, 2023 18:24:17.370917082 CET	80	49700	193.122.6.168	192.168.2.3
Feb 7, 2023 18:24:17.425228119 CET	49700	80	192.168.2.3	193.122.6.168
Feb 7, 2023 18:25:22.371258020 CET	80	49700	193.122.6.168	192.168.2.3
Feb 7, 2023 18:25:22.371350050 CET	49700	80	192.168.2.3	193.122.6.168
Feb 7, 2023 18:25:57.387985945 CET	49700	80	192.168.2.3	193.122.6.168
Feb 7, 2023 18:25:57.405881882 CET	80	49700	193.122.6.168	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 7, 2023 18:24:17.263358116 CET	58921	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:24:17.284573078 CET	53	58921	8.8.8.8	192.168.2.3
Feb 7, 2023 18:24:17.299715996 CET	62704	53	192.168.2.3	8.8.8.8
Feb 7, 2023 18:24:17.320004940 CET	53	62704	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 7, 2023 18:24:17.263358116 CET	192.168.2.3	8.8.8.8	0x6390	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.299715996 CET	192.168.2.3	8.8.8.8	0x6153	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)	false

DNS Answers

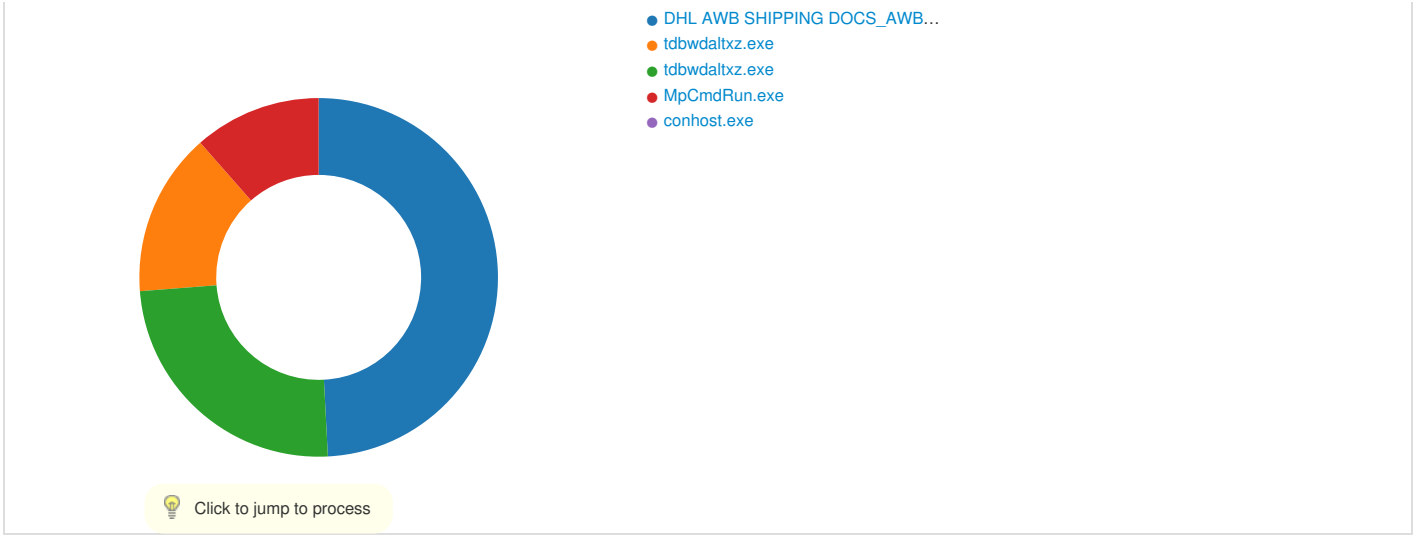
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 7, 2023 18:24:17.284573078 CET	8.8.8.8	192.168.2.3	0x6390	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:24:17.284573078 CET	8.8.8.8	192.168.2.3	0x6390	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.284573078 CET	8.8.8.8	192.168.2.3	0x6390	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.284573078 CET	8.8.8.8	192.168.2.3	0x6390	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.284573078 CET	8.8.8.8	192.168.2.3	0x6390	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.284573078 CET	8.8.8.8	192.168.2.3	0x6390	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.320004940 CET	8.8.8.8	192.168.2.3	0x6153	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)	false
Feb 7, 2023 18:24:17.320004940 CET	8.8.8.8	192.168.2.3	0x6153	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.320004940 CET	8.8.8.8	192.168.2.3	0x6153	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.320004940 CET	8.8.8.8	192.168.2.3	0x6153	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.320004940 CET	8.8.8.8	192.168.2.3	0x6153	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)	false
Feb 7, 2023 18:24:17.320004940 CET	8.8.8.8	192.168.2.3	0x6153	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- checkip.dyndns.org

Statistics

Behavior



System Behavior

Analysis Process: DHL AWB SHIPPING DOCS_AWB_0009123.exe PID: **1772**, Parent PID: **3452**

General

Target ID:	0
Start time:	18:24:09
Start date:	07/02/2023
Path:	C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe
Imagebase:	0x400000
File size:	459101 bytes
MD5 hash:	CF98F42B9D4BBDC20E54E7E0CA7543C0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsv9935.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsq9965.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsl9995.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW

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	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsl9995.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
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	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\wfpxt.ubj	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\rjnyysvx.m	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsv9935.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsl9995.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsq9965.tmp	0	29479	fd 39 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 03 00 00 00 fd 19 00 00 fd 00 00 00 fd 28 00 00 00 00 00 00 fd 38 00 00 01 00 00 00 6a 39 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 25 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	9,(8j9%	success or wait	19	406224	WriteFile
C:\Users\user\AppData\Local\Temp\wfpxt.ubj	0	16384	0b 6e 2b fd fd fd 00 fd 7b 1d 4b fd 75 fd 29 05 34 70 fd fd 19 fd 80 5d fd dc fd 07 fd 61 fd 27 fd 75 fd fd 7b fd 6e 20 42 57 36 fd 50 7f fd 3a fd fd 1f fd 59 fd fd 55 fd 09 50 f4 fd 11 fd fd 2f fd 3f fd 3c 60 41 fd fd fd 37 03 21 fd 6f 2d 5e 49 2c fd fd fd fd fd 54 fd 64 7f fd 71 fd fd 16 42 fd 31 fd fd fd fd fd 50 fd 42 fd 23 32 69 fd fd fd 2c fd 13 13 05 47 fd fd fd fd fd fd fd fd 2e 35 fd fd fd 70 17 fd fd 47 fd fd 42 79 fd 5a 66 02 fd 3c 63 35 fd fd 50 fd 03 fd fd fd 3c fd fd fd fd 34 74 fd fd fd 17 0e 10 5a fd 29 4b 49 21 4c 78 59 29 06 fd 37 38 30 fd 7a 54 fd fd 48 fd 38 69 fd fd 7d fd fd fd 38 fd 2a 6c fd 6d 28 fd fd fd fd fd fd 61 fd 37 fd fd 66 52 3a 31 70 52 0b 15 fd 0b fd 3c fd 52 fd 7c fd 3e 52 4d fd 1f	n+{Ku)4p]au{n BW6P:YUP/?<`A7!o- ^I,TdqB1PB#2,G.5pGByZ f<c5P<4t Z)KI!LxY)780zTH8i}8*Im(a7fR:pR<R|>RM	success or wait	15	406224	WriteFile
C:\Users\user\AppData\Local\Temp\rjnyysvx.m	0	5952	c6 30 30 35 6d fd fd 66 fd 46 3c fd 12 1b 30 35 6f fd 3a fd fd fd fd fd fd 3f 76 3e fd 33 fd 33 fd 3c fd 0c fd fd fd fd 4d fd 6b 6e 6c fd 30 32 61 fd fd 63 fd 45 3c fd 17 10 34 32 63 fd 20 fd fd fd fd fd fd 34 fd 44 36 33 fd 36 fd 33 fd 3f fd 0d fd fd fd 45 fd 67 6e 69 fd 35 33 50 fd 04 38 30 35 fd 70 38 fd 71 3f fd 32 fd 38 fd 75 20 fd 61 fd fd 62 65 61 62 6f fd 48 30 03 bb 76 0f fd 76 0c 40 33 fd 60 14 fd 69 2f 37 fd 70 14 36 fd 74 28 32 fd fd 67 31 7d 71 75 3c fd fd 47 2d fd 30 fd 33 fd 68 fd 66 fd fd fd 0f 77 38 4c 24 fd 6d fd 72 0b 44 3b 46 fd 07 fd 6f 6b 63 fd fd 6d fd 3b 34 fd 71 fd 3f fd 3c 40 fd 34 fd 30 fd fd fd 6d fd 73 75 3c 66 fd f1 fd 40 25 fd 60 34 fd fd 44 27 64 fd 4f 24 fd fd 41 35 1b fd 3d 01 fd 3c 72 fd	005mfF<05o:? v>33<Mknl02acE<42c 4D6363? Egni53P805p8q?28u abea boH0vv@3`i/7p6t(2g}u<G -03hfw8L $mrD;Fokcm;4q? <@40mu<f@%`4D'dO $A5=<r	success or wait	1	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 00 3f fd fd 44 5e fd 44 5e fd 44 5e 90 1b 3e fd 5f 5e 90 1b 3c fd 4e 5e 90 1b 3f fd 29 5e fd 44 5e fd fd 5e fd 29 48 fd 5d 5e fd 63 fd 3f fd 45 5e fd 63 fd 38 fd 45 5e fd 63 fd 3d fd 45 5e fd 52 69 63 68 44 5e fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 fd 01 fd 63 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 0b 00 00 fd 01	MZ@!L!This program cannot be run in DOS mode.$? D^D^D^>_^<N^?)^D^^)H]^c? E^c8E^c=E^RichD^PELc	success or wait	9	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe	unknown	512	success or wait	394	4061F5	ReadFile
C:\Users\user\Desktop\DHL AWB SHIPPING DOCS_AWB_0009123.exe	unknown	16384	success or wait	16	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsq9965.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsq9965.tmp	unknown	14722	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsq9965.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsq9965.tmp	unknown	16384	success or wait	25	4061F5	ReadFile

Analysis Process: tdbwdaltxz.exe PID: **5884**, Parent PID: **1772**

General

Target ID:	1
Start time:	18:24:10
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe" C:\Users\user\AppData\Local\Temp\rjnyysvx.m
Imagebase:	0x1060000
File size:	133120 bytes
MD5 hash:	377552A9A2C84B8C55314176A566C079
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_DotNetProcHook, Description: Detects executables with potential process hoocking, Source: 00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000001.00000002.262101627.0000000000ED0000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 23%, ReversingLabs • Detection: 13%, Virustotal, Browse

Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\rjnyysvx.m	unknown	4096	success or wait	1	1067102	ReadFile
C:\Users\user\AppData\Local\Temp\rjnyysvx.m	unknown	4096	success or wait	1	1067102	ReadFile
C:\Users\user\AppData\Local\Temp\wfpxt.ubj	unknown	210432	success or wait	1	5E0A1E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5E0F61	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5E0F61	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5E0F61	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5E0F61	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5E0F61	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	5E0F61	ReadFile

Analysis Process: tdbwdaltxz.exe

PID: **5864**, Parent PID: **5884**

General

Target ID:	2
Start time:	18:24:11
Start date:	07/02/2023
Path:	C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\tdbwdaltxz.exe
Imagebase:	0x1060000
File size:	133120 bytes
MD5 hash:	377552A9A2C84B8C55314176A566C079
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000002.00000002.520282991.0000000003C11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000002.00000002.520282991.0000000003C11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.520282991.0000000003C11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000002.00000002.520282991.0000000003C11000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000002.00000002.520282991.0000000003C11000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GenericDownloader_1, Description: Yara detected Generic Downloader, Source: 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_DotNetProcHook, Description: Detects executables with potential process hoocking, Source: 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000002.00000002.519555630.0000000001290000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: MAL_Envrial_Jan18_1, Description: Detects Encrial credential stealer malware, Source: 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: INDICATOR_SUSPICIOUS_EXE_DotNetProcHook, Description: Detects executables with potential process hoocking, Source: 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000002.00000002.518311344.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000002.00000002.519618240.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000002.00000002.519618240.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.519618240.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000002.00000002.519618240.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000002.00000002.519618240.0000000002B42000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000002.00000002.519032371.0000000000EE9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000002.00000002.519032371.0000000000EE9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000002.00000002.519032371.0000000000EE9000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000002.00000002.519032371.0000000000EE9000.00000004.00000020.00020000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_SnakeKeylogger_af3faa65, Description: unknown, Source: 00000002.00000002.519032371.0000000000EE9000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
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	72AECF06	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	72AECF06	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	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72AC5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72ACCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72A203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72A203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72AC5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71A31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71A31B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	49152	success or wait	1	71A31B4F	ReadFile

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: MpCmdRun.exe PID: **2576**, Parent PID: **5884**

General

Target ID:	12
Start time:	18:25:30
Start date:	07/02/2023
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable
Imagebase:	0x7ff618830000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	9968	182	0d 00 0a 00 0d 00 0a 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF61885BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10150	258	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 43 00 6f 00 6d 00 6d 00 61 00 6e 00 64 00 20 00 4c 00 69 00 6e 00 65 00 3a 00 20 00 22 00 43 00 3a 00 5c 00 50 00 72 00 6f 00 67 00 72 00 61 00 6d 00 20 00 46 00 69 00 6c 00 65 00 73 00 5c 00 57 00 69 00 6e 00 64 00 6f 00 77 00 73 00 20 00 44 00 65 00 66 00 65 00 6e 00 64 00 65 00 72 00 5c 00 6d 00 70 00 63 00 6d 00 64 00 72 00 75 00 6e 00 2e 00 65 00 78 00 65 00 22 00 20 00 2d 00 77 00 64 00 65 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00 20 00 53 00 74 00 61 00 72 00 74 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 75 00 65 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 30 00 37 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 31 00 38 00 3a 00 32 00 35 00 3a 00 33 00 30 00 0d 00 0a 00 0d	MpCmdRun: Command Line: "C:\Program Files\Windows Defender\mpcmdrun.exe" -wdenable Start Time: Tue Feb 07 2023 18:25:30	success or wait	1	7FF61885BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10408	86	4d 00 70 00 45 00 6e 00 73 00 75 00 72 00 65 00 50 00 72 00 6f 00 63 00 65 00 73 00 73 00 4d 00 69 00 74 00 69 00 67 00 61 00 74 00 69 00 6f 00 6e 00 50 00 6f 00 6c 00 69 00 63 00 79 00 3a 00 20 00 68 00 72 00 20 00 3d 00 20 00 30 00 78 00 31 00 0d 00 0a 00	MpEnsureProcessMitigationPolicy: hr = 0x1	success or wait	1	7FF61885BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10494	20	57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 0d 00 0a 00	WDEnable	success or wait	1	7FF61885BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10514	86	45 00 52 00 52 00 4f 00 52 00 3a 00 20 00 4d 00 70 00 57 00 44 00 45 00 6e 00 61 00 62 00 6c 00 65 00 28 00 54 00 52 00 55 00 45 00 29 00 20 00 66 00 61 00 69 00 6c 00 65 00 64 00 20 00 28 00 38 00 30 00 30 00 37 00 30 00 34 00 45 00 43 00 29 00 0d 00 0a 00	ERROR: MpWDEnable(TRUE) failed (800704EC)	success or wait	1	7FF61885BC96	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10600	100	4d 00 70 00 43 00 6d 00 64 00 52 00 75 00 6e 00 3a 00 20 00 45 00 6e 00 64 00 20 00 54 00 69 00 6d 00 65 00 3a 00 20 00 0e 20 54 00 75 00 65 00 20 00 0e 20 46 00 65 00 62 00 20 00 0e 20 30 00 37 00 20 00 0e 20 32 00 30 00 32 00 33 00 20 00 31 00 38 00 3a 00 32 00 35 00 3a 00 33 00 30 00 0d 00 0a 00	MpCmdRun: End Time: Tue Feb 07 2023 18:25:30	success or wait	1	7FF61885BC96	WriteFile
C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	10700	174	2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 2d 00 0d 00 0a 00	---	success or wait	1	7FF61885BC96	WriteFile

Analysis Process: conhost.exe PID: **6048**, Parent PID: **2576**

General

Target ID:	13
Start time:	18:25:30
Start date:	07/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly