ID: 502163
Sample Name: DHL AWB TRACKING DETAILS.exe
Cookbook: default.jbs
Time: 17:07:19
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

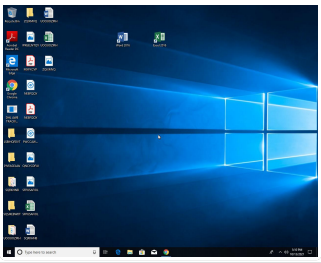
Windows Analysis Report DHL AWB TRACKING DETAIL…

Overview

General Information

Sample Name:	DHL AWB TRACKING DETAILS.exe
Analysis ID:	502163
MD5:	1fc9414612683fa..
SHA1:	780cee42ffebc33..
SHA256:	ae095ebb3fffa75…
Tags:	DHL exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

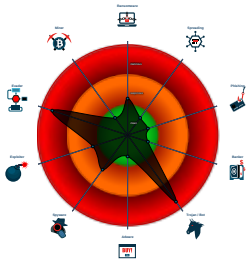
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Hides that the sample has been dow…
- Uses schtasks.exe or at.exe to add …
- Uses dynamic DNS services
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- DHL AWB TRACKING DETAILS.exe (PID: 2600 cmdline: 'C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe' MD5: 1FC9414612683FA9B525A75355706490)
  - schtasks.exe (PID: 3228 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWvcJacCRTJ' /XML 'C:\Users\user\AppData\Local\Temp\tmpA586.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHL AWB TRACKING DETAILS.exe (PID: 6228 cmdline: C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe MD5: 1FC9414612683FA9B525A75355706490)
    - schtasks.exe (PID: 6740 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp1FEB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6736 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6756 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp252C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6656 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- DHL AWB TRACKING DETAILS.exe (PID: 3080 cmdline: 'C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe' 0 MD5: 1FC9414612683FA9B525A75355706490)
  - schtasks.exe (PID: 6024 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWvcJacCRTJ' /XML 'C:\Users\user\AppData\Local\Temp\tmpD512.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - DHL AWB TRACKING DETAILS.exe (PID: 6004 cmdline: C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe MD5: 1FC9414612683FA9B525A75355706490)
- dhcpmon.exe (PID: 1692 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 1FC9414612683FA9B525A75355706490)
  - schtasks.exe (PID: 5972 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWvcJacCRTJ' /XML 'C:\Users\user\AppData\Local\Temp\tmpFE36.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5996 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 1FC9414612683FA9B525A75355706490)
- dhcpmon.exe (PID: 3480 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 1FC9414612683FA9B525A75355706490)
  - schtasks.exe (PID: 6772 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWvcJacCRTJ' /XML 'C:\Users\user\AppData\Local\Temp\tmp6D1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6916 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 3740 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 1FC9414612683FA9B525A75355706490)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.763527582.000000000293 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.941003643.0000000003FF 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.941003643.0000000003FF 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x43575:$a: NanoCore • 0x435ce:$a: NanoCore • 0x4360b:$a: NanoCore • 0x43684:$a: NanoCore • 0x56d2f:$a: NanoCore • 0x56d44:$a: NanoCore • 0x56d79:$a: NanoCore • 0x6fd3b:$a: NanoCore • 0x6fd50:$a: NanoCore • 0x6fd85:$a: NanoCore • 0x435d7:$b: ClientPlugin • 0x43614:$b: ClientPlugin • 0x43f12:$b: ClientPlugin • 0x43f1f:$b: ClientPlugin • 0x56aeb:$b: ClientPlugin • 0x56b06:$b: ClientPlugin • 0x56b36:$b: ClientPlugin • 0x56d4d:$b: ClientPlugin • 0x56d82:$b: ClientPlugin • 0x6faf7:$b: ClientPlugin • 0x6fb12:$b: ClientPlugin
00000004.00000002.942709422.000000000599 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000004.00000002.942709422.000000000599 0000.00000004.00020000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
Click to see the 54 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.dhcpmon.exe.39b1f58.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
12.2.dhcpmon.exe.39b1f58.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
12.2.dhcpmon.exe.39b1f58.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
12.2.dhcpmon.exe.39b1f58.4.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
4.2.DHL AWB TRACKING DETAILS.exe.40405cc .4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
Click to see the 61 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

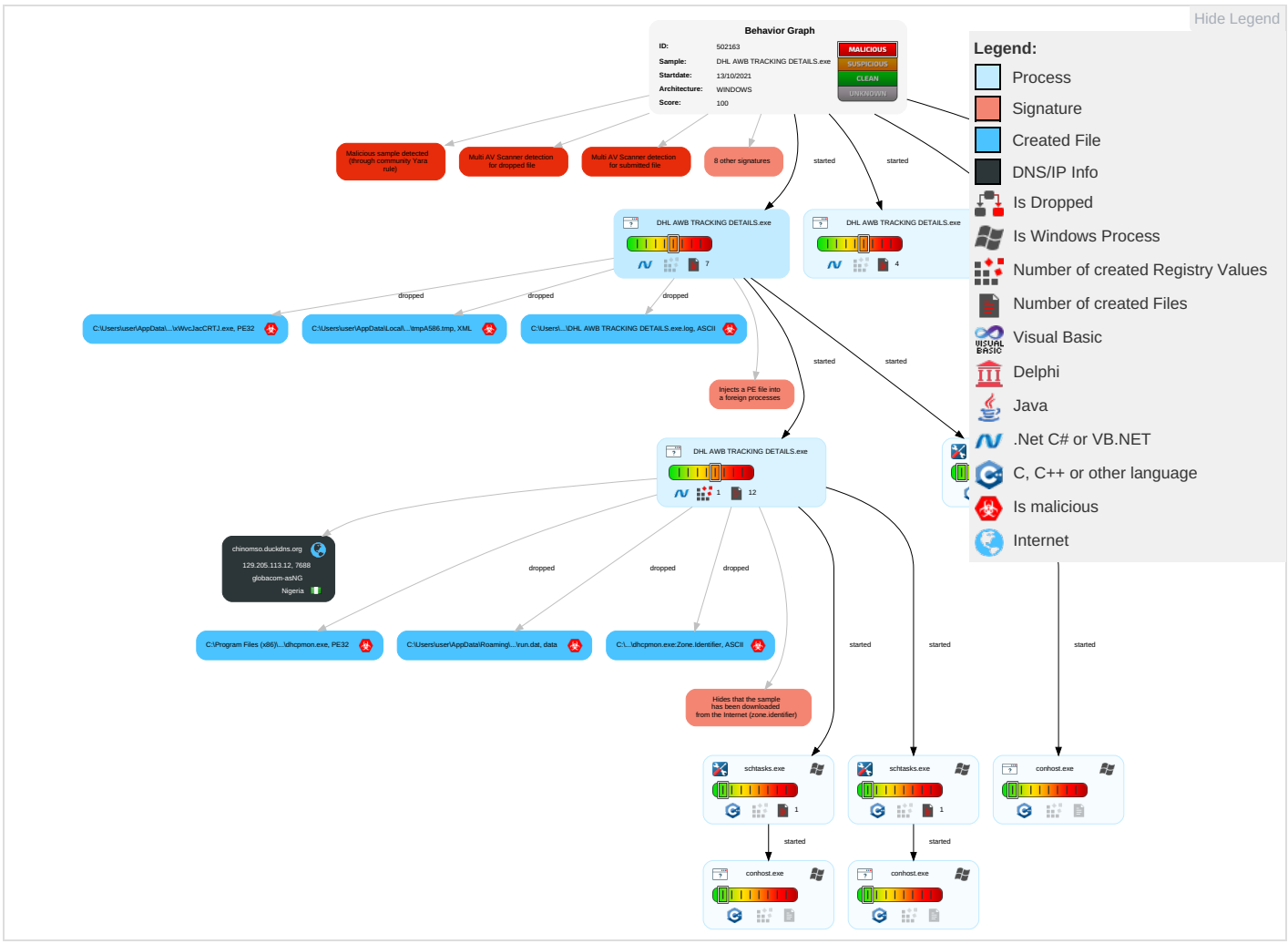
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 2 1	Query Registry 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc

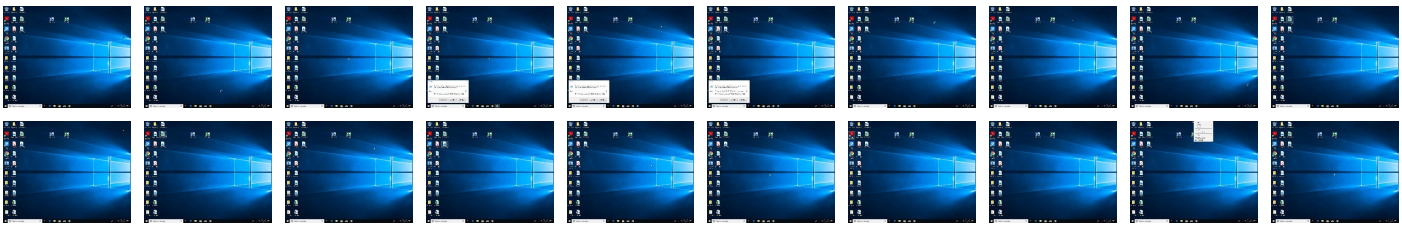
Behavior Graph



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 TRACKING DETAILS.exe	30%	Virustotal		Browse
DHL AWB TRACKING DETAILS.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	30%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\xWvcJacCRTJ.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.DHL AWB TRACKING DETAILS.exe.5990000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
4.2.DHL AWB TRACKING DETAILS.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	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://go.microsoft.c.r	0%	Avira URL Cloud	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
chinomso.duckdns.org	129.205.113.12	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
129.205.113.12	chinomso.duckdns.org	Nigeria		37148	globacom-asNG	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502163
Start date:	13.10.2021
Start time:	17:07:19
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL AWB TRACKING DETAILS.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:	34
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@30/12@6/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 77.5% • Quality standard deviation: 17.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:08:27	API Interceptor	883x Sleep call for process: DHL AWB TRACKING DETAILS.exe modified
17:08:41	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe" s>$(Arg0)
17:08:41	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
17:08:44	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
17:08:46	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	651776
Entropy (8bit):	7.645296007215276
Encrypted:	false
SSDEEP:	12288:o0cPk+EcPRnhUVjfP+Uuf2j613ztwXUoaAE0UErHPsRIY9Zi6g6SB:JcPhEcpw+U02e13ztwXUoaAlrvsxi6aB
MD5:	1FC9414612683FA9B525A75355706490
SHA1:	780CEE42FFEBC33391E0A814DB98E5CF8AFFED5E
SHA-256:	AE095EBB3FFFA75296B6DB100D55EF0DCF8E8C7EB9A0C616E0ADB732DC4EE8C9
SHA-512:	87777CA70B286FDB5B769EFAB741A09546E68825769B381328E8DEB9321099A5315A30CBF512CACD3297BB1F7CD55983048AEB15C47862A4811BCE2A6BF4DBEB
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 30%, Browse • Antivirus: ReversingLabs, Detection: 36%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....yfa.....0..... ... .@.. .....`..... ..@.....P...O.... ..(.....@..... ..... ..H.....text..... ..... ..`.rsrc...(.... .....@..@.rel oc.....@.....@..B.....H.....C..t{.....@....E.....".(....*....0.....|....(.....+..*....0.....|.....(.....(&....*...0.....{....l#... ...o@[.+..*..0..W.....#.....?.....,.#.....?...+..#.....,..#.....#.....o@Z.}.....(&....*..0.....{....+..*.0.....}....*....0.....(....(l....+..*....0.....,.....(-.....+...(.....*....0.....{.....+..*.0..C.....,...(.....(.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL AWB TRACKING DETAILS.exe.log	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp252C.tmp	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp6D1.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGztn:cbhK79lNQR/rydbz9l3YODOLNdq3c
MD5:	98538A364A3BA38F686CD7300023F6F3
SHA1:	A7448453C818945E0EE9F3B3DF5C9DBBB3908B08
SHA-256:	32A23EDC35BA2651543B0A153DF21A74365487C55D25342F2D50AAD9BAC4C6E9
SHA-512:	B097B2D8A7C66A4EF8E9080F2BE0EE8757340FAB89B154C2DEB0C25AA8EDD043A08065D527CABE29AF35398B5C4E1E9F5A96018493372301899A968FF0B8D8F9
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpA586.tmp	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped

C:\Users\user\AppData\Local\Temp\tmpA586.tmp	
Size (bytes):	1644
Entropy (8bit):	5.184496115167584
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGztn:cbhK79lNQR/rydbz9I3YODOLNdq3c
MD5:	98538A364A3BA38F686CD7300023F6F3
SHA1:	A7448453C818945E0EE9F3B3DF5C9DBBB3908B08
SHA-256:	32A23EDC35BA2651543B0A153DF21A74365487C55D25342F2D50AAD9BAC4C6E9
SHA-512:	B097B2D8A7C66A4EF8E9080F2BE0EE8757340FAB89B154C2DEB0C25AA8EDD043A08065D527CABE29AF35398B5C4E1E9F5A960184933723018 99A968FF0B8D8F9
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpD512.tmp	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.184496115167584
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGztn:cbhK79lNQR/rydbz9I3YODOLNdq3c
MD5:	98538A364A3BA38F686CD7300023F6F3
SHA1:	A7448453C818945E0EE9F3B3DF5C9DBBB3908B08
SHA-256:	32A23EDC35BA2651543B0A153DF21A74365487C55D25342F2D50AAD9BAC4C6E9
SHA-512:	B097B2D8A7C66A4EF8E9080F2BE0EE8757340FAB89B154C2DEB0C25AA8EDD043A08065D527CABE29AF35398B5C4E1E9F5A960184933723018 99A968FF0B8D8F9
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpFE36.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.184496115167584
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGztn:cbhK79lNQR/rydbz9I3YODOLNdq3c
MD5:	98538A364A3BA38F686CD7300023F6F3
SHA1:	A7448453C818945E0EE9F3B3DF5C9DBBB3908B08
SHA-256:	32A23EDC35BA2651543B0A153DF21A74365487C55D25342F2D50AAD9BAC4C6E9
SHA-512:	B097B2D8A7C66A4EF8E9080F2BE0EE8757340FAB89B154C2DEB0C25AA8EDD043A08065D527CABE29AF35398B5C4E1E9F5A960184933723018 99A968FF0B8D8F9
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	data
Category:	dropped
Size (bytes):	8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:z4Lwn:U0n
MD5:	EB318F2FBFAD576CC3C0E6AF2BC1422E
SHA1:	4DCF1FBDAC8D7F275708497533F634FA9455DEC5
SHA-256:	7D340406A2A1DBE171C2D222B76249FFB7AE1710FA2EA414DBE56F3EA91A1246
SHA-512:	945198CF5156ABE8EBD4F173DE7121E6BE983E6019A593E6AA61718F6FF8374610B0CB9257B199E4782FAED40473A14302BDDCD27082CDDCBB70742DE530ECE5
Malicious:	**true**
Reputation:	unknown
Preview:	...U[..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	51
Entropy (8bit):	4.655282146267042
Encrypted:	false
SSDEEP:	3:oNt+WfWhtrkynLmsribiC:oNwvU0Lb2b/
MD5:	36CF5F6A15460E47553697F3171A68A2
SHA1:	664885AA8C10A6C8D4C997C7A1B4D9451B7B41D6
SHA-256:	BB464FA713EA5DD09CCC34D69C6F641D78142D8A780759E274911734BC3BD689
SHA-512:	69CCE61DFE05023576CD1CC98CA449FFEA4EF145050A018B6E1E0238413A797C0BE6CF82D87A7778E7B6470603B2112D2D9A6513B4B6B1932D0B44AF482832A
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe

C:\Users\user\AppData\Roaming\xWvcJacCRTJ.exe	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	651776
Entropy (8bit):	7.645296007215276
Encrypted:	false
SSDEEP:	12288:o0cPk+EcPRnhUVjfP+Uuf2j613ztwXUoaAE0UErHPsRIY9Zi6g6SB:JcPhEcpw+U02e13ztwXUoaAlrvsxi6aB
MD5:	1FC9414612683FA9B525A75355706490
SHA1:	780CEE42FFEBC33391E0A814DB98E5CF8AFFED5E
SHA-256:	AE095EBB3FFFA75296B6DB100D55EF0DCF8E8C7EB9A0C616E0ADB732DC4EE8C9
SHA-512:	87777CA70B286FDB5B769EFAB741A09546E68825769B381328E8DEB9321099A5315A30CBF512CACD3297BB1F7CD55983048AEB15C47862A4811BCE2A6BF4DBEB
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 36%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....yfa.....0..... ... .@.. .....`..... ..@.....P...O.... ..(.....@..... ..... ..H.....text..... ..... ..`.rsrc...(.... .....@..@.rel oc.....@.....@..B.....H.....C..t{.....@....E.....".(.....*....0.....|....(.....+..*....0.....|.....(.....(&....*...0.....{....l#... ...o@[.+..*..0..W.....#.....?.....,#.....?...+..#.....,.#.....#.....o@Z.}.....(&....*..0.....{.....+..*.0.....}.....*....0.....(....(l....+..*....0.....,.....(-.....+...(.....*....0.....{.....+..*.0..C.....,...(.....(.....

C:\Users\user\AppData\Roaming\xWvcJacCRTJ.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Roaming\xWvcJacCRTJ.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.645296007215276
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	DHL AWB TRACKING DETAILS.exe
File size:	651776
MD5:	1fc9414612683fa9b525a75355706490
SHA1:	780cee42ffebc33391e0a814db98e5cf8affed5e
SHA256:	ae095ebb3fffa75296b6db100d55ef0dcf8e8c7eb9a0c616e0adb732dc4ee8c9
SHA512:	87777ca70b286fdb5b769efab741a09546e68825769b381328e8deb9321099a5315a30cbf512cacd3297bb1f7cd55983048aeb15c47862a4811bce2a6bf4dbeb
SSDEEP:	12288:o0cPk+EcPRnhUVjfP+Uuf2j613ztwXUoaAE0UErHPsRIY9Zi6g6SB:JcPhEcpw+U02e13ztwXUoaAlrvsxi6aB
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....yfa.....0..... ... .@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a04a2
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x616679B9 [Wed Oct 13 06:16:25 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9e4a8	0x9e600	False	0.854562327348	data	7.65420629233	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x628	0x800	False	0.33984375	data	3.48748935924	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa4000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-17:08:43.476938	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54531	8.8.8.8	192.168.2.4
10/13/21-17:09:21.017276	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49257	8.8.8.8	192.168.2.4
10/13/21-17:09:39.305371	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55854	8.8.8.8	192.168.2.4
10/13/21-17:10:15.196557	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61721	8.8.8.8	192.168.2.4

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 17:08:43.363162041 CEST	192.168.2.4	8.8.8.8	0x9a24	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 17:09:02.149257898 CEST	192.168.2.4	8.8.8.8	0xeb16	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 17:09:20.903023958 CEST	192.168.2.4	8.8.8.8	0x23cc	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 17:09:39.191277981 CEST	192.168.2.4	8.8.8.8	0x2224	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 17:09:57.858398914 CEST	192.168.2.4	8.8.8.8	0x6385	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)
Oct 13, 2021 17:10:15.082997084 CEST	192.168.2.4	8.8.8.8	0xd0b0	Standard query (0)	chinomso.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 17:08:43.476938009 CEST	8.8.8.8	192.168.2.4	0x9a24	No error (0)	chinomso.duckdns.org		129.205.113.12	A (IP address)	IN (0x0001)
Oct 13, 2021 17:09:02.165541887 CEST	8.8.8.8	192.168.2.4	0xeb16	No error (0)	chinomso.duckdns.org		129.205.113.12	A (IP address)	IN (0x0001)
Oct 13, 2021 17:09:21.017276049 CEST	8.8.8.8	192.168.2.4	0x23cc	No error (0)	chinomso.duckdns.org		129.205.113.12	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 17:09:39.305371046 CEST	8.8.8.8	192.168.2.4	0x2224	No error (0)	chinomso.duckdns.org		129.205.113.12	A (IP address)	IN (0x0001)
Oct 13, 2021 17:09:57.876790047 CEST	8.8.8.8	192.168.2.4	0x6385	No error (0)	chinomso.duckdns.org		129.205.113.12	A (IP address)	IN (0x0001)
Oct 13, 2021 17:10:15.196557045 CEST	8.8.8.8	192.168.2.4	0xd0b0	No error (0)	chinomso.duckdns.org		129.205.113.12	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: DHL AWB TRACKING DETAILS.exe PID: 2600 Parent PID: 5840

General

Start time:	17:08:19
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe'
Imagebase:	0xec0000
File size:	651776 bytes
MD5 hash:	1FC9414612683FA9B525A75355706490
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: 00000001.00000002.707807684.0000000003312000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.707666257.00000000032D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.708348717.00000000042D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.708348717.00000000042D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.708348717.00000000042D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3228 Parent PID: 2600

General

Start time:	17:08:34
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\xWvcJacCRTJ' /XML 'C:\Users\user\AppData\Local\Temp\tmpA586.tmp'
Imagebase:	0x920000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities — Show Windows behavior

Analysis Process: conhost.exe PID: 4100 Parent PID: 3228

General

Start time:	17:08:35
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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 AWB TRACKING DETAILS.exe PID: 6228 Parent PID: 2600

General

Start time:	17:08:35
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
Imagebase:	0xa70000
File size:	651776 bytes
MD5 hash:	1FC9414612683FA9B525A75355706490
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.941003643.0000000003FF9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.941003643.0000000003FF9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.942709422.0000000005990000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.942709422.0000000005990000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.942709422.0000000005990000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.942404493.00000000057F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.942404493.00000000057F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.937316619.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.937316619.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.937316619.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.939950156.0000000002FF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 6740 Parent PID: 6228

General

Start time:	17:08:39
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp1FEB.tmp'
Imagebase:	0x920000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6736 Parent PID: 6740

General

Start time:	17:08:39
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: schtasks.exe PID: 6756 Parent PID: 6228

General

Start time:	17:08:41
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp252C.tmp'
Imagebase:	0x920000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6656 Parent PID: 6756

General

Start time:	17:08:41
Start date:	13/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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 AWB TRACKING DETAILS.exe PID: 3080 Parent PID: 968

General

Start time:	17:08:41
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL AWB TRACKING DETAILS.exe' 0
Imagebase:	0x160000
File size:	651776 bytes
MD5 hash:	1FC9414612683FA9B525A75355706490
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: 00000009.00000002.747751155.0000000002570000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000009.00000002.747672827.0000000002531000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.748402227.0000000003539000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.748402227.0000000003539000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.748402227.0000000003539000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 1692 Parent PID: 968

General

Start time:	17:08:44
Start date:	13/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xe60000
File size:	651776 bytes
MD5 hash:	1FC9414612683FA9B525A75355706490
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: 0000000A.00000002.753079815.0000000003310000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.752990326.00000000032D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.754436217.00000000042D9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.754436217.00000000042D9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.754436217.00000000042D9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 30%, Virustotal, Browse • Detection: 36%, ReversingLabs

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: dhcpmon.exe PID: 3480 Parent PID: 3424

General

Start time:	17:08:50
Start date:	13/10/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x490000
File size:	651776 bytes
MD5 hash:	1FC9414612683FA9B525A75355706490
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: 0000000C.00000002.763527582.0000000002931000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000C.00000002.763599855.0000000002970000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.764189899.0000000003939000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.764189899.0000000003939000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.764189899.0000000003939000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis