ID: 344428
Sample Name: DHL-#AWB130501923096PDF.exe
Cookbook: default.jbs
Time: 15:24:02
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

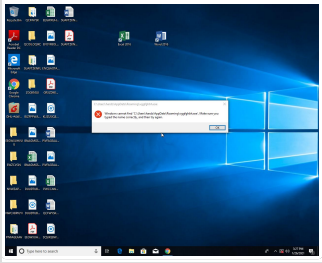
Analysis Report DHL-#AWB130501923096PDF.exe

Overview

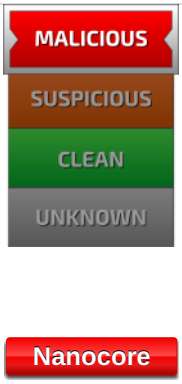
General Information

Sample Name:	DHL-#AWB130501923096PDF.exe
Analysis ID:	344428
MD5:	13e8443bf19ea58.
SHA1:	62ae36fa6f7d5a2..
SHA256:	1372611a622074..
Tags:	exe NanoCore

Most interesting Screenshot:



Detection



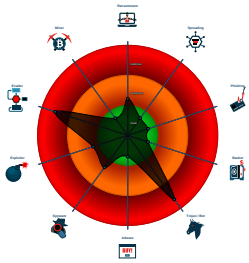
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Startup

- **System is w10x64**
- DHL-#AWB130501923096PDF.exe (PID: 5464 cmdline: 'C:\Users\user\Desktop\DHL-#AWB130501923096PDF.exe' MD5: 13E8443BF19EA588B2C7A77251746FE8)
  - cmd.exe (PID: 1968 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'sweddf' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\vggfghbh.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6016 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 5952 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'sweddf' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\vggfghbh.exe' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - vggfghbh.exe (PID: 7044 cmdline: 'C:\Users\user\AppData\Roaming\vggfghbh.exe' MD5: 13E8443BF19EA588B2C7A77251746FE8)
    - InstallUtil.exe (PID: 6204 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "185.162.88.26",
    "185.162.88.26:2091"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000002.605338854.000000000531 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
00000016.00000002.605338854.000000000531 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000016.00000002.605485890.00000000053C 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000016.00000002.605485890.00000000053C 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000016.00000002.605485890.00000000053C 0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 28 entries				

Unpacked PEs

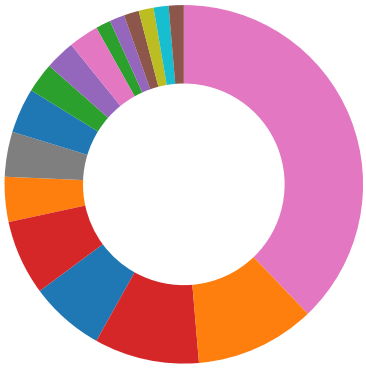
Source	Rule	Description	Author	Strings
22.2.InstallUtil.exe.5310000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
22.2.InstallUtil.exe.5310000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
22.2.InstallUtil.exe.53c0000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
22.2.InstallUtil.exe.53c0000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
22.2.InstallUtil.exe.53c0000.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 7 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Compliance:

Uses 32bit PE files

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

Binary contains paths to debug symbols

Networking:

C2 URLs / IPs found in malware configuration

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

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 AntiVM_3

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

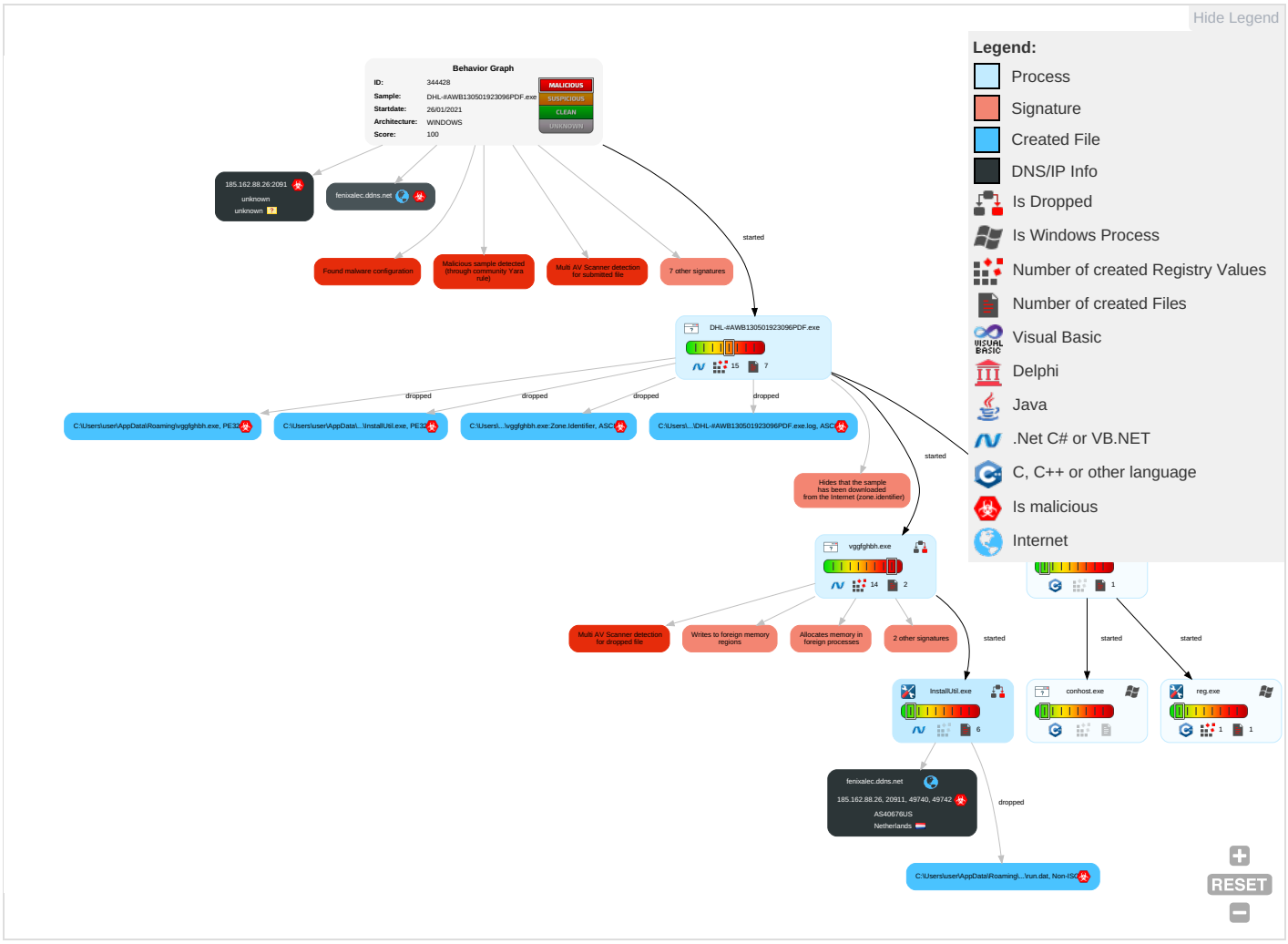
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Com and
Valid Accounts 1	Windows Management Instrumentation	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encr Char
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Non- Port
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Rem Softv
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 1 1	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non- Appli Laye Proto
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Virtualization/Sandbox Evasion 3	SSH	Keylogging	Data Transfer Size Limits	Appli Laye Proto
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multi Com
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Com Used
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Appli Laye
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Virtualization/Sandbox Evasion 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 3 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Proto
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail

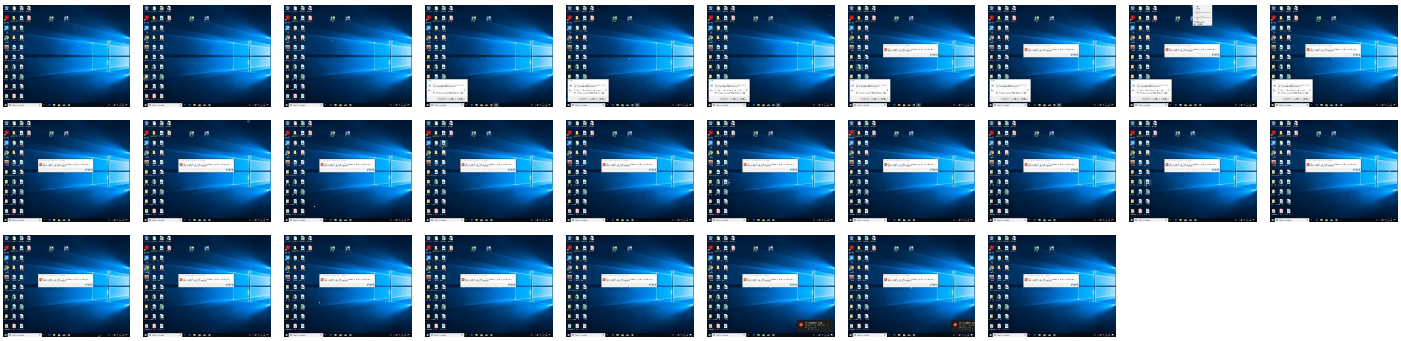
Behavior Graph

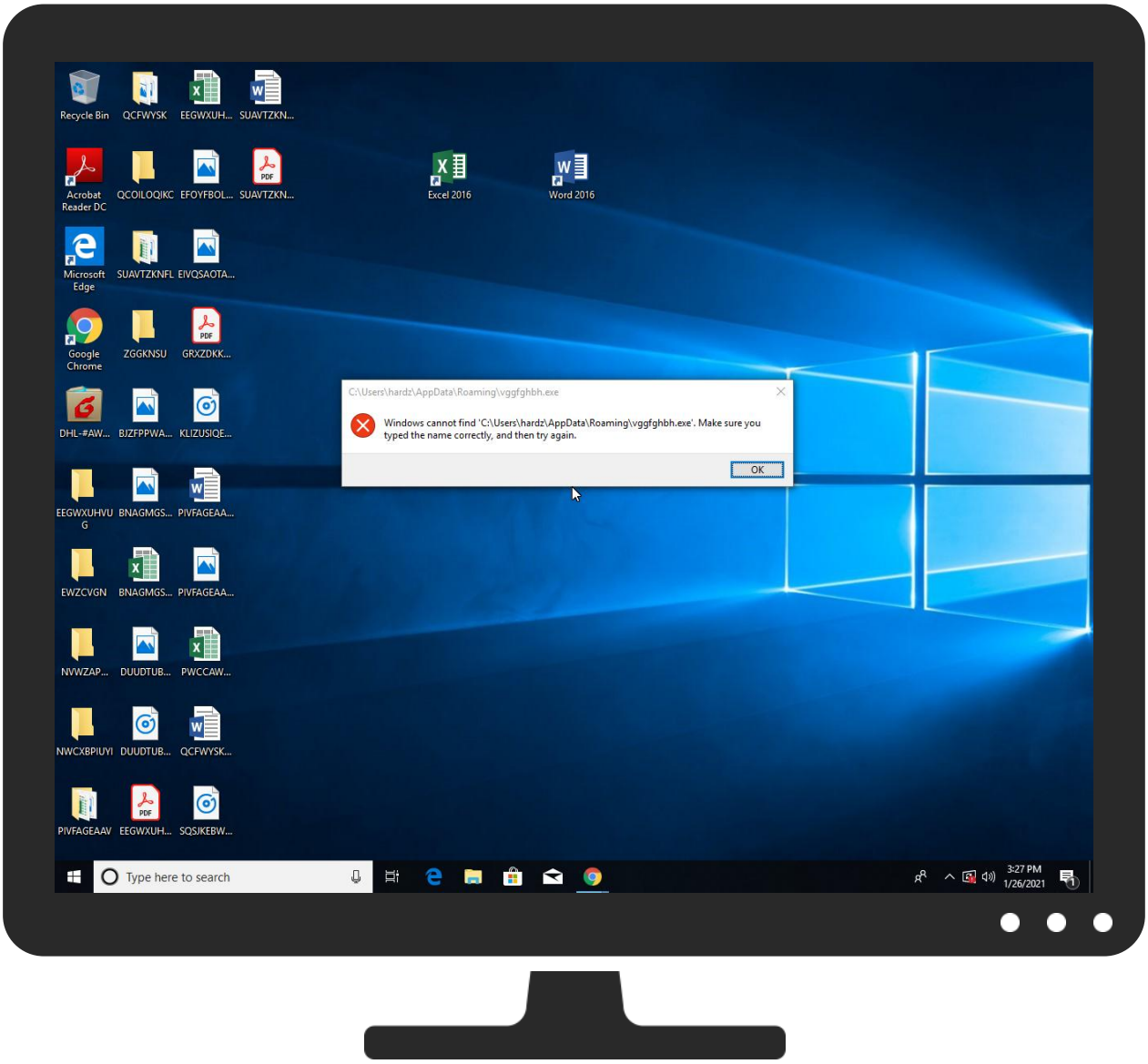


Screenshots

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-#AWB130501923096PDF.exe	51%	Virustotal		Browse
DHL-#AWB130501923096PDF.exe	50%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\vggfghbh.exe	50%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.2.InstallUtil.exe.53c0000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://ns.adb	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://ns.adobe.c/g	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://ocsp.pki.goog/gsr202	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ns.adobe.cobj	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://ocsp.pki.goog/gts1o1core0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	
http://ns.ado/1	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

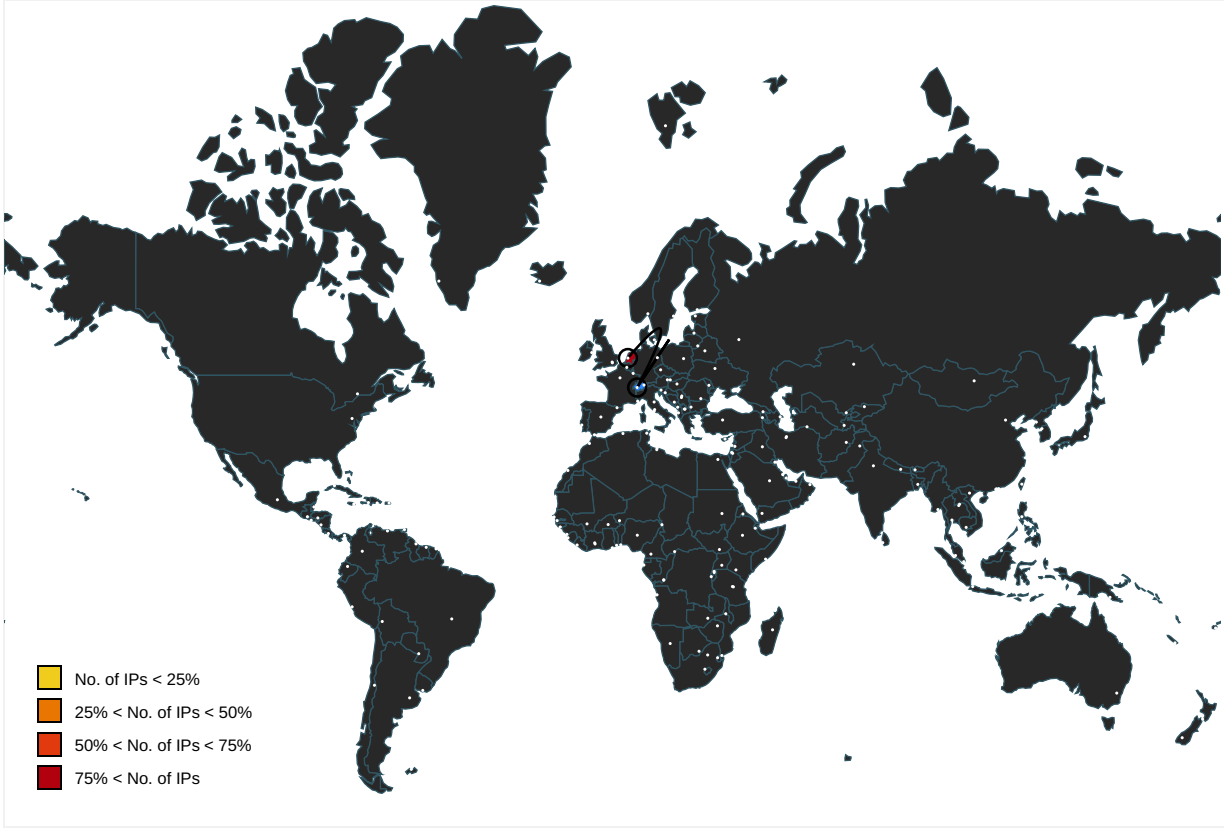
Name	IP	Active	Malicious	Antivirus Detection	Reputation
fenixalec.ddns.net	185.162.88.26	true	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.adb	DHL-#AWB130501923096PDF.exe, 00000000.00000003.219214900.0000000008ED1000.00000004.00000001.sdmp, vggfghbh.exe, 00000012.00000002.607947015.00000000089F0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki.goog/gsr2/GTS1O1.crt0	DHL-#AWB130501923096PDF.exe, 00000000.00000002.324232114.0000000001472000.00000004.00000020.sdmp, vggfghbh.exe, 00000012.00000002.595684941.0000000002C7F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.c/g	DHL-#AWB130501923096PDF.exe, 00000000.00000003.323063383.0000000008EE0000.00000004.00000001.sdmp, DHL-#AWB130501923096PDF.exe, 00000000.00000003.219214900.0000000008ED1000.00000004.00000001.sdmp, vggfghbh.exe, 00000012.00000002.607947015.00000000089F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.pki.goog/gsr2/gsr2.crl0?	DHL-#AWB130501923096PDF.exe, 00000000.00000002.324232114.0000000001472000.00000004.00000020.sdmp, vggfghbh.exe, 00000012.00000002.593981212.0000000000F07000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gsr202	DHL-#AWB130501923096PDF.exe, 00000000.00000002.324232114.0000000001472000.00000004.00000020.sdmp, vggfghbh.exe, 00000012.00000002.593981212.0000000000F07000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	DHL-#AWB130501923096PDF.exe, 00000000.00000002.324232114.0000000001472000.00000004.00000020.sdmp, vggfghbh.exe, 00000012.00000002.593981212.0000000000F07000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.adobe.cobj	DHL-#AWB130501923096PDF.exe, 00000000.00000003.323063383.0000008EE0000.00000004.00000001.sdmp, DHL-#AWB130501923096PDF.exe, 00000000.00000003.219214900.0000000008ED1000.00000004.00000001.sdmp, vggfghbh.exe, 00000012.00000002.607947015.000000089F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.pki.goog/gts1o1core0	DHL-#AWB130501923096PDF.exe, 00000000.00000002.324232114.0000000001472000.00000004.00000020.sdmp, vggfghbh.exe, 00000012.00000002.595684941.0000000002C7F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	DHL-#AWB130501923096PDF.exe, 00000000.00000002.324710955.0000002FE1000.00000004.00000001.sdmp, vggfghbh.exe, 00000012.00000002.595604258.0000000002C51000.00000004.00000001.sdmp	false		high
http://schema.org/WebPage	vggfghbh.exe, 00000012.00000002.595684941.0000000002C7F000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	DHL-#AWB130501923096PDF.exe, 00000000.00000002.324232114.0000000001472000.00000004.00000020.sdmp, vggfghbh.exe, 00000012.00000002.595684941.0000000002C7F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ns.ado/1	DHL-#AWB130501923096PDF.exe, 00000000.00000003.323063383.0000008EE0000.00000004.00000001.sdmp, DHL-#AWB130501923096PDF.exe, 00000000.00000003.219214900.0000000008ED1000.00000004.00000001.sdmp, vggfghbh.exe, 00000012.00000002.607947015.000000089F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.162.88.26:2091	unknown	unknown		unknown	unknown	true
185.162.88.26	unknown	Netherlands		40676	AS40676US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344428
Start date:	26.01.2021
Start time:	15:24:02
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL-#AWB130501923096PDF.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:	32
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/5@9/2
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.3%) • Quality average: 37.8% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.139.144, 13.88.21.125, 172.217.23.36, 52.255.188.83, 23.210.248.85, 51.104.139.180, 95.101.22.224, 95.101.22.216, 8.248.139.254, 67.27.157.254, 8.248.141.254, 8.241.9.254, 67.26.83.254, 20.54.26.129, 52.155.217.156 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, www.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, auto.au.download.windowsupdate.com.c.footprint.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, db3p-ris-pf-prod-atm.trafficmanager.net, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
15:25:02	API Interceptor	193x Sleep call for process: DHL-#AWB130501923096PDF.exe modified
15:25:06	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run sweddf C:\Users\user\AppData\Roaming\vggfghbh.exe
15:25:14	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run sweddf C:\Users\user\AppData\Roaming\vggfghbh.exe
15:25:54	API Interceptor	176x Sleep call for process: vggfghbh.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.162.88.26	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	
	PO#4018-308875.exe	Get hash	malicious	Browse	
	PO#4018-308875.exe	Get hash	malicious	Browse	
	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	
	MEDUSI492126.pdf.exe	Get hash	malicious	Browse	
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
fenixalec.ddns.net	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	PO#4018-308875.exe	Get hash	malicious	Browse	• 185.162.88.26
	PO#4018-308875.exe	Get hash	malicious	Browse	• 185.162.88.26
	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	MEDUSI492126.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS40676US	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	PO#4018-308875.exe	Get hash	malicious	Browse	• 185.162.88.26
	PO#4018-308875.exe	Get hash	malicious	Browse	• 185.162.88.26
	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Ulma9B5jo1.exe	Get hash	malicious	Browse	• 104.149.57.92
	MEDUSI492126.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Request for Quotation.exe	Get hash	malicious	Browse	• 45.34.249.53
	silkOrder00110.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Order_BC012356.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	Document#20014464370.pdf.exe	Get hash	malicious	Browse	• 185.162.88.26
	t1XJOlYvhExZyrm.exe	Get hash	malicious	Browse	• 104.225.208.15
	SWIFT_COPY00993Payment_advic4555pdf.exe	Get hash	malicious	Browse	• 172.106.11 1.244
	QN08qH1zYv.exe	Get hash	malicious	Browse	• 104.149.57.92
	SWIFT-COPY Payment advice3243343.exe	Get hash	malicious	Browse	• 172.106.11 1.244
	catalogo TAWI group.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Rfq 214871_TAWI Catalog.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Rfq_Catalog.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	NPD76122.exe	Get hash	malicious	Browse	• 104.217.23 1.247
	h3dFAROdF3.exe	Get hash	malicious	Browse	• 104.217.23 1.248
	d2mISAbTQN.exe	Get hash	malicious	Browse	• 104.217.23 1.248

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	IMG_1677.EXE	Get hash	malicious	Browse	
	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	
	file.exe	Get hash	malicious	Browse	
	IMG_5371.EXE	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	file.exe	Get hash	malicious	Browse	
	IMG_9501.EXE	Get hash	malicious	Browse	
	IMG_04017.pdf.exe	Get hash	malicious	Browse	
	GFS_03781.xls.exe	Get hash	malicious	Browse	
	SPpfYOx5Ju.exe	Get hash	malicious	Browse	
	PO#4018-308875.exe	Get hash	malicious	Browse	
	PO#4018-308875.exe	Get hash	malicious	Browse	
	IMG_57880.pdf.exe	Get hash	malicious	Browse	
	PO 67542 PDF.exe	Get hash	malicious	Browse	
	Mi9eI6wu1p.exe	Get hash	malicious	Browse	
	OJ4zX7G77Y.exe	Get hash	malicious	Browse	
	IMG_50781.pdf.exe	Get hash	malicious	Browse	
	IMG_25579.pdf.exe	Get hash	malicious	Browse	
	IMG_40317.pdf.exe	Get hash	malicious	Browse	
	PO#4018-308875.pdf.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.509.8504.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL-#AWB130501923096PDF.exe.log

Process:	C:\Users\user\Desktop\DHL-#AWB130501923096PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1873
Entropy (8bit):	5.355036985457214
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjovitHoxHhAHKzvr1qHj:iqXeqm00YqhQnouRqjoKtlxHeqzTwD
MD5:	CDA95282F22F47DA2FDDC9E912B67FEF
SHA1:	67A40582A092B5DF40C3EB61A361A2D336FC69E0
SHA-256:	179E50F31095D0CFA13DCBB9CED6DEE424DFE8CEF8E05BDE1F840273F45E5F49
SHA-512:	1D151D92AE982D2149C2255826C2FFB89A475A1EB9B9FE93DC3706F3016CD6B309743B36A4D7F6D68F48CE25391FDA7A2BAE42061535EEA7862460424A3A2036
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

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

Process:	C:\Users\user\Desktop\DHL-#AWB130501923096PDF.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	41064
Entropy (8bit):	6.164873449128079
Encrypted:	false
SSDEEP:	384:FtpFVLK0MsihB9VKS7xdgE7KJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+sPZTd:ZBMs2SqdD86Iq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

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

Joe Sandbox View:	• Filename: IMG_1677.EXE, Detection: malicious, Browse • Filename: PO#4018-308875.pdf.exe, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: IMG_5371.EXE, Detection: malicious, Browse • Filename: file.exe, Detection: malicious, Browse • Filename: IMG_9501.EXE, Detection: malicious, Browse • Filename: IMG_04017.pdf.exe, Detection: malicious, Browse • Filename: GFS_03781.xls.exe, Detection: malicious, Browse • Filename: SPpfYOx5Ju.exe, Detection: malicious, Browse • Filename: PO#4018-308875.exe, Detection: malicious, Browse • Filename: PO#4018-308875.exe, Detection: malicious, Browse • Filename: IMG_57880.pdf.exe, Detection: malicious, Browse • Filename: PO 67542 PDF.exe, Detection: malicious, Browse • Filename: Mi9el6wu1p.exe, Detection: malicious, Browse • Filename: OJ4zX7G77Y.exe, Detection: malicious, Browse • Filename: IMG_50781.pdf.exe, Detection: malicious, Browse • Filename: IMG_25579.pdf.exe, Detection: malicious, Browse • Filename: IMG_40317.pdf.exe, Detection: malicious, Browse • Filename: PO#4018-308875.pdf.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.509.8504.exe, Detection: malicious, Browse
Reputation:	moderate, very likely benign file
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..T.....r... .....@.. ....`.....4r..O.....b..h>.....p..... ..... ..H.....text....R... ...T..... ..`.rsrc.....V.....@..@.rel oc.....`.....@..B.....hr.....H.....".|J.....lm.....o.....2~.....o...*.r...p(....*VrK..p(....s.....*..0.....(....(....o....o....(....o.... .....T(....o....(....o....o ...o!....4(....o....(....o....o ...o".....(....rm..ps#...o....($.....(%....o&....ry..p.....%.r...p.%.(.....(....('....((.....o)...('.....*.*.....".(*...*..{Q...-...}Q.....(+...(....(,....(+...*"..(- ...*..(....*..(.....r...p.(/...o0...s....}T...*....0.. .....~S...-.s

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:769tn:mPn
MD5:	6DEA3729E0EE0DF26AAF5F581C872ABD
SHA1:	5841F8EA23E50C046B215C7093F79F947C97F512
SHA-256:	E6A34F967491141207F04D69188778A7B1700B5D64B5E84B6BEBFD09C7B43F10
SHA-512:	FDCCBE4AECFD43551DA75F7BE3828D2AF245DA3616CB98C10275146EEA0B04899381249FED2F4389238777FB7E5007C32D71729DB0550FC0ED32751B62F9225
Malicious:	**true**
Reputation:	low
Preview:	..$.Q..H

C:\Users\user\AppData\Roaming\vggfghbh.exe

Process:	C:\Users\user\Desktop\DHL-#AWB130501923096PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	729600
Entropy (8bit):	5.487518327344531
Encrypted:	false
SSDEEP:	12288:ynIAmIvHfNbxp0GZnfNtSyv71xiqZV/HZ25:EIAms/HZnFn1xietHZ2
MD5:	13E8443BF19EA588B2C7A77251746FE8
SHA1:	62AE36FA6F7D5A21E026A8BBEBED94BAC81384E6
SHA-256:	1372611A622074319850 55EA8ECB4121B3DFB199E615102C06CC38E5AABDD65D
SHA-512:	0DBCF414E821C737084E2D3CC378F5E8DE1920AB2D41340D5C474316A051001F71CB47F0733CB588923D885455137C2B36993CAECB160333BC23E539B9DB6DE
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 50%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....*..... ... .@.. ..... .`.....H...S.... ..V&.....`..... ....H.....text..... ....`.rsrc...V&... ...(.....@..@.relo c.....`..... .....@..B.....H.....@....*.....O.....[.....2."..2.`..Y.X.....D...A.....C. .N..O..p.$.{....4."...I.$.I.O..).2...k.../....2.v...m.9.i.O..1. 9...I.".X.A....v...k.=./....5.%...a.(.n.O..$.v...m.%.a....f.!...f.%.f.....#.>.....+.#...,z).(.....+L#<.=.8.....C.B...i~ixi.u.,.,.,".I.l.l.p.....).....b.c.n....J.J.J.V.(.(.(.&..... ....~$.$o$.8.K.K.K.E.T.T.T.H.w.w.w.Z.Z.Z.u.F.K`.a.v.....-.|.}.

C:\Users\user\AppData\Roaming\vggfghbh.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\DHL-#AWB130501923096PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26

C:\Users\user\AppData\Roaming\vggfghbh.exe:Zone.Identifier	
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.487518327344531
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	DHL-#AWB130501923096PDF.exe
File size:	729600
MD5:	13e8443bf19ea588b2c7a77251746fe8
SHA1:	62ae36fa6f7d5a21e026a8bbebed94bac81384e6
SHA256:	1372611a62207431985055ea8ecb4121b3dfb199e615102c06cc38e5aabdd65d
SHA512:	0dbcf414e821c737084e2d3cc378f5e8de1920ab2d41340d5c474316a051001f71cb47f0733cb588923d885455137c2b36993caecb160333bc23e539b9db6de9
SSDEEP:	12288:ynIAmIvHfNbxp0GZnfNtSyv71xiqZV/HZ25:EIAms/HZnFn1xietHZ2
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....*..... ... .@.. .....`.....

File Icon

Icon Hash:	d8aa9a8e96968eb2

Static PE Info

General

Entrypoint:	0x4a159e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT, HIGH_ENTROPY_VA
Time Stamp:	0x1B1180D7 [Wed May 23 03:45:27 1984 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4

General

File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa1548	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa2000	0x12656	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xb6000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9f5a4	0x9f600	False	0.525298713235	data	5.34593586049	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa2000	0x12656	0x12800	False	0.266456397804	data	5.87092786486	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb6000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa2250	0x8a8	data		
RT_ICON	0xa2af8	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0xa3060	0x94a8	data		
RT_ICON	0xac508	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 254, next used block 4294967055		
RT_ICON	0xb0730	0x25a8	data		
RT_ICON	0xb2cd8	0x10a8	data		
RT_ICON	0xb3d80	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xb41e8	0x68	data		
RT_VERSION	0xb4250	0x21c	data	Chinese	China
RT_MANIFEST	0xb446c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
LegalCopyright	Copyright(C) 2015-2020 Tencent. All Rights Reserved
ProductVersion	7.2.19.158
FileVersion	7.2.19.158
FileDescription	Foxmail
Translation	0x0804 0x03a8

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	China	

Network Behavior

Network Port Distribution

Total Packets: 93

- 53 (DNS)
- 20911 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 15:26:32.845701933 CET	49740	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:33.184623003 CET	20911	49740	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:33.690479994 CET	49740	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:34.064266920 CET	20911	49740	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:34.565557003 CET	49740	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:34.811480045 CET	20911	49740	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:38.879782915 CET	49742	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:39.050628901 CET	20911	49742	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:39.550419092 CET	49742	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:39.724929094 CET	20911	49742	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:40.237946033 CET	49742	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:40.412484884 CET	20911	49742	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:44.427333117 CET	49744	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:44.595402002 CET	20911	49744	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:45.097647905 CET	49744	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:45.267420053 CET	20911	49744	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:45.769571066 CET	49744	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:45.940321922 CET	20911	49744	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:50.451677084 CET	49745	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:50.637541056 CET	20911	49745	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:51.145010948 CET	49745	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:51.322264910 CET	20911	49745	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:51.833287001 CET	49745	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:52.003298998 CET	20911	49745	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:56.101031065 CET	49746	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:56.274370909 CET	20911	49746	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:56.786196947 CET	49746	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:56.955404997 CET	20911	49746	185.162.88.26	192.168.2.3
Jan 26, 2021 15:26:57.458051920 CET	49746	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:26:57.628541946 CET	20911	49746	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:02.887914896 CET	49747	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:03.059770107 CET	20911	49747	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:03.567929983 CET	49747	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:03.759299040 CET	20911	49747	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:04.271156073 CET	49747	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:04.452070951 CET	20911	49747	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:08.460773945 CET	49748	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:08.636281013 CET	20911	49748	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:09.146486998 CET	49748	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:09.322979927 CET	20911	49748	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:09.834032059 CET	49748	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:10.005353928 CET	20911	49748	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:14.024635077 CET	49749	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:14.206463099 CET	20911	49749	185.162.88.26	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 15:27:14.709430933 CET	49749	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:14.890496969 CET	20911	49749	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:15.396995068 CET	49749	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:15.577440023 CET	20911	49749	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:19.586685896 CET	49750	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:19.758215904 CET	20911	49750	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:20.272365093 CET	49750	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:20.451981068 CET	20911	49750	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:20.959933043 CET	49750	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:21.132288933 CET	20911	49750	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:25.776262999 CET	49751	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:25.949553967 CET	20911	49751	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:26.461123943 CET	49751	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:26.634459972 CET	20911	49751	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:27.148838043 CET	49751	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:27.317351103 CET	20911	49751	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:31.417654037 CET	49752	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:31.620445013 CET	20911	49752	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:32.132900000 CET	49752	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:32.322252989 CET	20911	49752	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:32.836074114 CET	49752	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:33.135557890 CET	20911	49752	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:37.242897987 CET	49753	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:37.415766001 CET	20911	49753	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:37.923605919 CET	49753	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:38.092448950 CET	20911	49753	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:38.620318890 CET	49753	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:38.792669058 CET	20911	49753	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:42.825841904 CET	49758	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:43.005439043 CET	20911	49758	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:43.555794954 CET	49758	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:43.728413105 CET	20911	49758	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:44.359241962 CET	49758	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:44.535487890 CET	20911	49758	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:48.556391001 CET	49765	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:48.803752899 CET	20911	49765	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:49.313306093 CET	49765	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:49.484812975 CET	20911	49765	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:50.015961885 CET	49765	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:50.332370996 CET	20911	49765	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:54.345803976 CET	49766	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:54.522444010 CET	20911	49766	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:55.032967091 CET	49766	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:55.214257002 CET	20911	49766	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:55.719532967 CET	49766	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:27:55.894716024 CET	20911	49766	185.162.88.26	192.168.2.3
Jan 26, 2021 15:27:59.971550941 CET	49767	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:28:00.140594959 CET	20911	49767	185.162.88.26	192.168.2.3
Jan 26, 2021 15:28:00.641827106 CET	49767	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:28:01.010138035 CET	20911	49767	185.162.88.26	192.168.2.3
Jan 26, 2021 15:28:01.517283916 CET	49767	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:28:01.687365055 CET	20911	49767	185.162.88.26	192.168.2.3
Jan 26, 2021 15:28:05.769408941 CET	49768	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:28:05.939847946 CET	20911	49768	185.162.88.26	192.168.2.3
Jan 26, 2021 15:28:06.454822063 CET	49768	20911	192.168.2.3	185.162.88.26
Jan 26, 2021 15:28:06.630326033 CET	20911	49768	185.162.88.26	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 15:24:51.004863977 CET	64185	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:24:51.052695990 CET	53	64185	8.8.8.8	192.168.2.3
Jan 26, 2021 15:24:51.936860085 CET	65110	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:24:51.984791040 CET	53	65110	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 15:24:53.826543093 CET	58361	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:24:53.874450922 CET	53	58361	8.8.8.8	192.168.2.3
Jan 26, 2021 15:24:55.349008083 CET	63492	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:24:55.399744987 CET	53	63492	8.8.8.8	192.168.2.3
Jan 26, 2021 15:24:57.140198946 CET	60831	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:24:57.201503992 CET	53	60831	8.8.8.8	192.168.2.3
Jan 26, 2021 15:24:57.424484968 CET	60100	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:24:57.483562946 CET	53	60100	8.8.8.8	192.168.2.3
Jan 26, 2021 15:24:58.490983009 CET	53195	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:24:58.539068937 CET	53	53195	8.8.8.8	192.168.2.3
Jan 26, 2021 15:24:59.427931070 CET	50141	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:24:59.479903936 CET	53	50141	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:00.378860950 CET	53023	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:00.426603079 CET	53	53023	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:01.322943926 CET	49563	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:01.370829105 CET	53	49563	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:02.205514908 CET	51352	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:02.262638092 CET	53	51352	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:05.022424936 CET	59349	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:05.070317030 CET	53	59349	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:05.799045086 CET	57084	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:05.846967936 CET	53	57084	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:06.617281914 CET	58823	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:06.668586016 CET	53	58823	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:19.756206989 CET	57568	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:19.814055920 CET	53	57568	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:23.925025940 CET	50540	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:23.975766897 CET	53	50540	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:35.989748955 CET	54366	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:36.048000097 CET	53	54366	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:38.849658966 CET	53034	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:38.900736094 CET	53	53034	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:48.913367987 CET	57762	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:48.969801903 CET	53	57762	8.8.8.8	192.168.2.3
Jan 26, 2021 15:25:54.724850893 CET	55435	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:25:54.796421051 CET	53	55435	8.8.8.8	192.168.2.3
Jan 26, 2021 15:26:01.806772947 CET	50713	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:26:01.857460022 CET	53	50713	8.8.8.8	192.168.2.3
Jan 26, 2021 15:26:06.749186039 CET	56132	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:26:06.816737890 CET	53	56132	8.8.8.8	192.168.2.3
Jan 26, 2021 15:26:37.744086981 CET	58987	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:26:37.792056084 CET	53	58987	8.8.8.8	192.168.2.3
Jan 26, 2021 15:26:40.731296062 CET	56579	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:26:40.787782907 CET	53	56579	8.8.8.8	192.168.2.3
Jan 26, 2021 15:26:50.390696049 CET	60633	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:26:50.448775053 CET	53	60633	8.8.8.8	192.168.2.3
Jan 26, 2021 15:26:56.040361881 CET	61292	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:26:56.098870039 CET	53	61292	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:02.821433067 CET	63619	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:02.877702951 CET	53	63619	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:25.705291033 CET	64938	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:25.761727095 CET	53	64938	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:31.328788042 CET	61946	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:31.387881994 CET	53	61946	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:37.158355951 CET	64910	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:37.214723110 CET	53	64910	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:40.337074041 CET	52123	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:40.387881041 CET	53	52123	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:41.053005934 CET	56130	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:41.112512112 CET	53	56130	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:41.787533998 CET	56338	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:41.835544109 CET	53	56338	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:42.510091066 CET	59420	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:42.557867050 CET	53	59420	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 15:27:43.160180092 CET	58784	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:43.208003044 CET	53	58784	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:43.871534109 CET	63978	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:43.919646025 CET	53	63978	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:44.750557899 CET	62938	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:44.809628963 CET	53	62938	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:45.884926081 CET	55708	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:45.942502022 CET	53	55708	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:47.086849928 CET	56803	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:47.143177986 CET	53	56803	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:47.673472881 CET	57145	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:47.721323013 CET	53	57145	8.8.8.8	192.168.2.3
Jan 26, 2021 15:27:59.909024000 CET	55359	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:27:59.969980001 CET	53	55359	8.8.8.8	192.168.2.3
Jan 26, 2021 15:28:05.705981970 CET	58306	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:28:05.768352985 CET	53	58306	8.8.8.8	192.168.2.3
Jan 26, 2021 15:28:11.331341028 CET	64124	53	192.168.2.3	8.8.8.8
Jan 26, 2021 15:28:11.379264116 CET	53	64124	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 15:26:50.390696049 CET	192.168.2.3	8.8.8.8	0x98a6	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 15:26:56.040361881 CET	192.168.2.3	8.8.8.8	0x73fe	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:02.821433067 CET	192.168.2.3	8.8.8.8	0x3cae	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:25.705291033 CET	192.168.2.3	8.8.8.8	0xe979	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:31.328788042 CET	192.168.2.3	8.8.8.8	0xa840	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:37.158355951 CET	192.168.2.3	8.8.8.8	0x427d	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:59.909024000 CET	192.168.2.3	8.8.8.8	0xfb0e	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 15:28:05.705981970 CET	192.168.2.3	8.8.8.8	0xf275	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 15:28:11.331341028 CET	192.168.2.3	8.8.8.8	0x936f	Standard query (0)	fenixalec.ddns.net	A (IP address)	IN (0x0001)

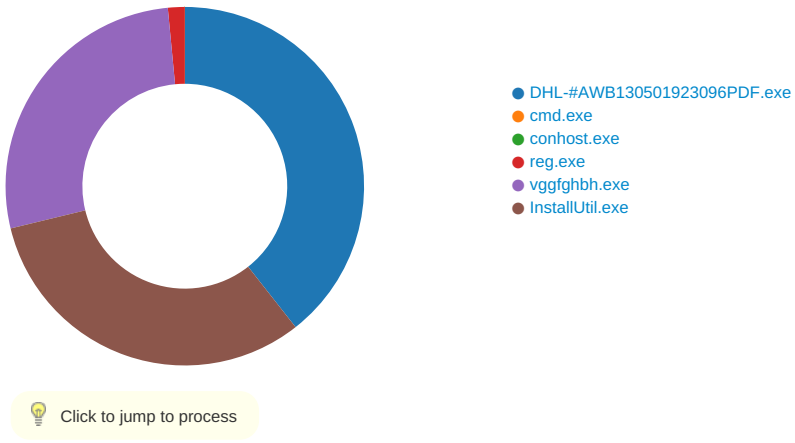
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 15:26:50.448775053 CET	8.8.8.8	192.168.2.3	0x98a6	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 26, 2021 15:26:56.098870039 CET	8.8.8.8	192.168.2.3	0x73fe	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:02.877702951 CET	8.8.8.8	192.168.2.3	0x3cae	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:25.761727095 CET	8.8.8.8	192.168.2.3	0xe979	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:31.387881994 CET	8.8.8.8	192.168.2.3	0xa840	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:37.214723110 CET	8.8.8.8	192.168.2.3	0x427d	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 26, 2021 15:27:59.969980001 CET	8.8.8.8	192.168.2.3	0xfb0e	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 26, 2021 15:28:05.768352985 CET	8.8.8.8	192.168.2.3	0xf275	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)
Jan 26, 2021 15:28:11.379264116 CET	8.8.8.8	192.168.2.3	0x936f	No error (0)	fenixalec.ddns.net		185.162.88.26	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: DHL-#AWB130501923096PDF.exe PID: 5464 Parent PID: 5648

General

Start time:	15:24:55
Start date:	26/01/2021
Path:	C:\Users\user\Desktop\DHL-#AWB130501923096PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL-#AWB130501923096PDF.exe'
Imagebase:	0xc20000
File size:	729600 bytes
MD5 hash:	13E8443BF19EA588B2C7A77251746FE8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.326369360.0000000004937000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.326369360.0000000004937000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.326369360.0000000004937000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.328448374.0000000004ACD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.328448374.0000000004ACD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.328448374.0000000004ACD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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	6E0ECF06	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	6E0ECF06	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	568F1E3	CopyFileExW
C:\Users\user\AppData\Roaming\vggfghbh.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | synchronous io non alert | non directory file	success or wait	1	568F1E3	CopyFileExW
C:\Users\user\AppData\Roaming\vggfghbh.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	568F1E3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL-#AWB130501923096PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0	41064	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 07 5a 8e 5a 00 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 54 00 00 00 0c 00 00 00 00 00 00 86 72 00 00 00 20 00 00 00 80 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 c0 00 00 00 02 00 00 9a 80 01 00 03 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@...... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....Z.Z.......... ....0..T...........r... ....@.. ....`................	success or wait	1	568F1E3	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\vggfghbh.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 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 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 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 50 45 00 00 4c 01 03 00 d7 80 11 1b 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 f6 09 00 00 2a 01 00 00 00 00 00 9e 15 0a 00 00 20 00 00 00 20 0a 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 80 0b 00 00 02 00 00 00 00 00 00 02 00 60 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L................. ....*........... ... .@.. ....`................	success or wait	3	568F1E3	CopyFileExW
C:\Users\user\AppData\Roaming\vggfghbh.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	568F1E3	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL-#AWB130501923096PDF.exe.log	unknown	1873	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 50 72 65 73 65 6e 74 61 74 69 6f 6e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..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..3,"PresentationCore, Version=	success or wait	1	6E3FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	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	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 1968 Parent PID: 5464

General

Start time:	15:25:00
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'sweddf' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\vggfghbh.exe'
Imagebase:	0xbd0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6016 Parent PID: 1968

General

Start time:	15:25:01
Start date:	26/01/2021
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: reg.exe PID: 5952 Parent PID: 1968

General

Start time:	15:25:01
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows\CurrentVersion\Run' /f /v 'sweddf' /t REG_SZ /d 'C:\Users\user\AppData\Roaming\vggfghbh.exe'
Imagebase:	0x8c0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	sweddf	unicode	C:\Users\user\AppData\Roaming\vggfghbh.exe	success or wait	1	8C5A1D	RegSetValueExW

Analysis Process: vggfghbh.exe PID: 7044 Parent PID: 5464

General

Start time:	15:25:46
Start date:	26/01/2021
Path:	C:\Users\user\AppData\Roaming\vggfghbh.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\vggfghbh.exe'
Imagebase:	0x850000
File size:	729600 bytes
MD5 hash:	13E8443BF19EA588B2C7A77251746FE8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.605435037.000000000473C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.605435037.000000000473C000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.605435037.000000000473C000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.605142766.00000000045A6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.605142766.00000000045A6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.605142766.00000000045A6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 50%, ReversingLabs
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	6E0ECF06	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	6E0ECF06	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	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: InstallUtil.exe PID: 6204 Parent PID: 7044

General

Start time:	15:26:24
Start date:	26/01/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x6d0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.605338854.0000000005310000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000016.00000002.605338854.0000000005310000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.605485890.00000000053C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000016.00000002.605485890.00000000053C0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.605485890.00000000053C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.591464383.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.591464383.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.591464383.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.601866891.0000000003BD9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.601866891.0000000003BD9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

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	6E0ECF06	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	6E0ECF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF3BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF31E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF3BEFF	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	f6 92 24 d0 51 c2 d8 48	..$.Q..H	success or wait	1	6CF31B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	4096	success or wait	1	6E0AD72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	512	success or wait	1	6E0AD72F	unknown

Disassembly

Code Analysis