ID: 336532
Sample Name: DHL_file 187652345643476245.exe
Cookbook: default.jbs
Time: 09:25:12
Date: 06/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

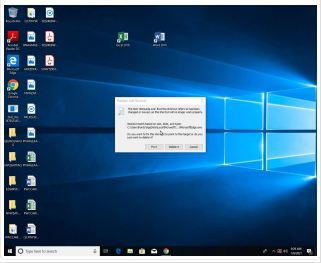
Analysis Report DHL_file 187652345643476245.exe

Overview

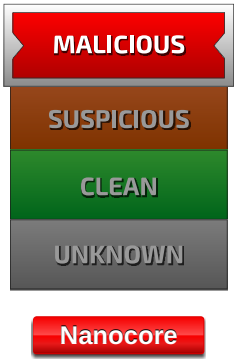
General Information

Sample Name:	DHL_file 187652345643476245.exe
Analysis ID:	336532
MD5:	303e92008ea45a..
SHA1:	29ff646c7c04a2b..
SHA256:	c4dbec4c0df381c..
Tags:	DHL exe Hostwinds NanoCore RAT

Most interesting Screenshot:



Detection

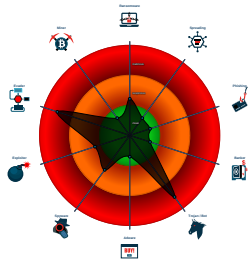


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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…
- Binary contains a suspicious time st…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- DHL_file 187652345643476245.exe (PID: 6652 cmdline: 'C:\Users\user\Desktop\DHL_file 187652345643476245.exe' MD5: 303E92008EA45ABDE4FC35D8D176015D)
  - demiusda.exe (PID: 1240 cmdline: 'C:\Users\user\AppData\Roaming\demiusda.exe' MD5: 303E92008EA45ABDE4FC35D8D176015D)
    - AddInProcess32.exe (PID: 1256 cmdline: C:\Users\user\AppData\Local\Temp\AddInProcess32.exe MD5: F2A47587431C466535F3C3D3427724BE)
    - watchprcss.exe (PID: 5164 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - watchprcss.exe (PID: 6304 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - watchprcss.exe (PID: 5712 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - watchprcss.exe (PID: 5404 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - watchprcss.exe (PID: 6660 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - watchprcss.exe (PID: 5024 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - watchprcss.exe (PID: 4076 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - watchprcss.exe (PID: 6508 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - watchprcss.exe (PID: 7020 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - watchprcss.exe (PID: 476 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - watchprcss.exe (PID: 6284 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - watchprcss.exe (PID: 1724 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - watchprcss.exe (PID: 7040 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - watchprcss.exe (PID: 3032 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
    - watchprcss.exe (PID: 7000 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
      - watchprcss.exe (PID: 6216 cmdline: 'C:\Users\user\AppData\Local\Temp\watchprcss.exe' MD5: 0E362E7005823D0BEC3719B902ED6D62)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "185.157.160.233",
    "105.112.113.90"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.624186822.000000000561 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000011.00000002.624186822.000000000561 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
00000011.00000002.620217311.0000000003F1 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000011.00000002.620217311.0000000003F1 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2f25:$a: NanoCore • 0x2f7e:$a: NanoCore • 0x2fbb:$a: NanoCore • 0x3034:$a: NanoCore • 0x166df:$a: NanoCore • 0x166f4:$a: NanoCore • 0x16729:$a: NanoCore • 0x2f1a3:$a: NanoCore • 0x2f1b8:$a: NanoCore • 0x2f1ed:$a: NanoCore • 0x2f87:$b: ClientPlugin • 0x2fc4:$b: ClientPlugin • 0x38c2:$b: ClientPlugin • 0x38cf:$b: ClientPlugin • 0x1649b:$b: ClientPlugin • 0x164b6:$b: ClientPlugin • 0x164e6:$b: ClientPlugin • 0x166fd:$b: ClientPlugin • 0x16732:$b: ClientPlugin • 0x2ef5f:$b: ClientPlugin • 0x2ef7a:$b: ClientPlugin
0000000C.00000002.623749902.000000000423 1000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1043d:$x1: NanoCore.ClientPluginHost • 0x1047a:$x2: IClientNetworkHost • 0x13fad:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 22 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.2.AddInProcess32.exe.5a80000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
17.2.AddInProcess32.exe.5a80000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
17.2.AddInProcess32.exe.5a80000.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
17.2.AddInProcess32.exe.5610000.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
17.2.AddInProcess32.exe.5610000.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
Click to see the 7 entries				

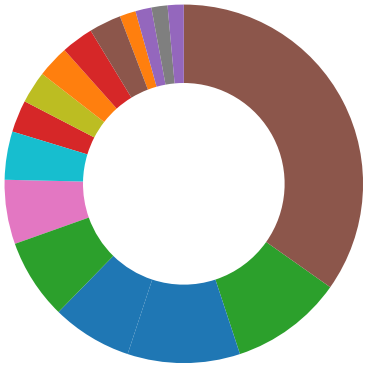
Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview

- AV Detection
- 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

Networking:

- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker
- Binary contains a suspicious time stamp

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:

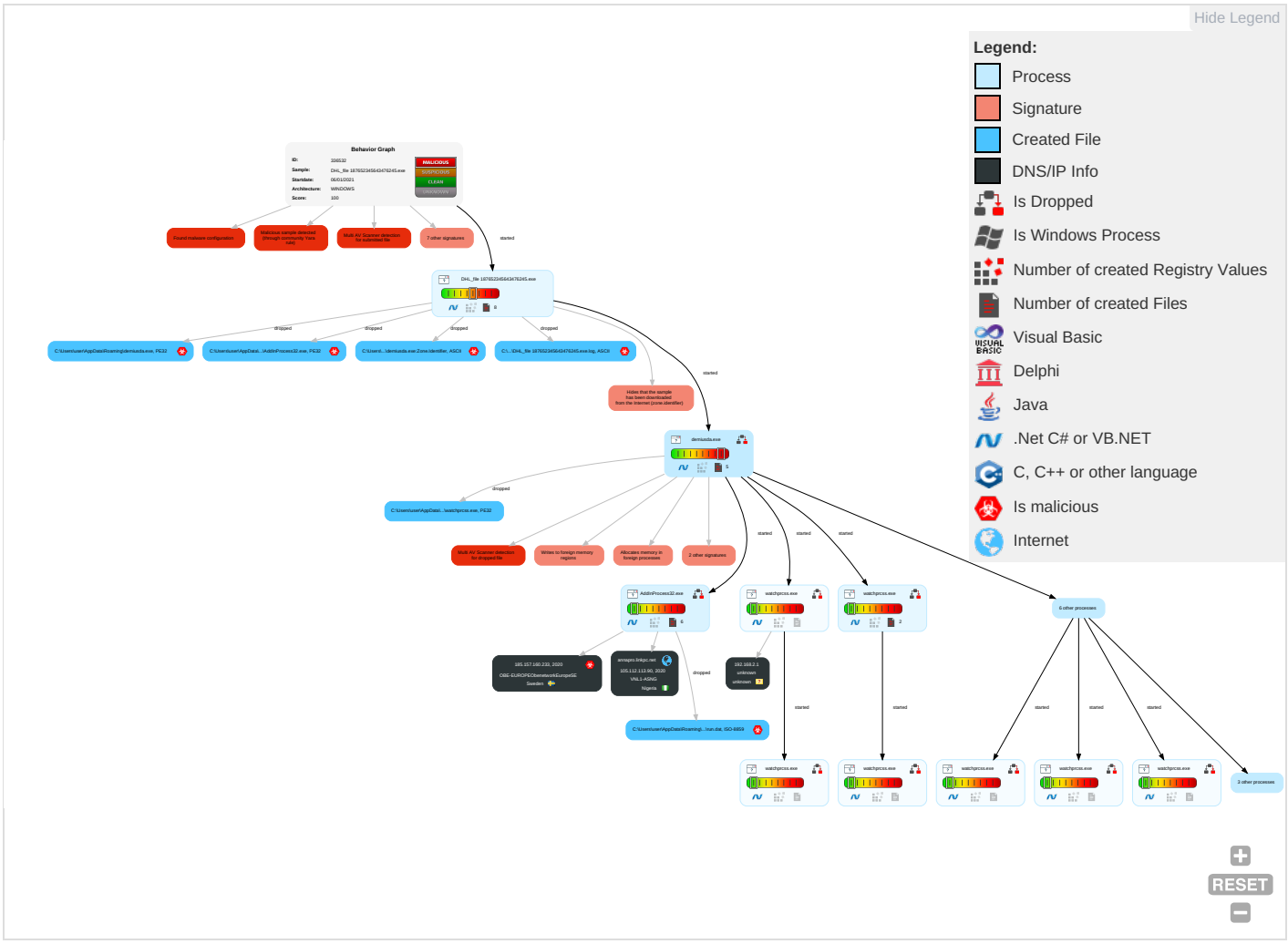
Detected Nanocore Rat

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	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	Input Capture 2 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	Valid Accounts 1	Valid Accounts 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	Non- Port
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Obfuscated Files or Information 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Rem Softw
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 3 1 2	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	Registry Run Keys / Startup Folder 2	Timestomp 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	Masquerading 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	Valid Accounts 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	Network Service Scanning	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_file 187652345643476245.exe	23%	ReversingLabs	Win32.Trojan.Pwsx	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\watchprcss.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\demiusda.exe	23%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.AddInProcess32.exe.5a80000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
17.2.AddInProcess32.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://iptc.tc4xmp:	0%	Avira URL Cloud	safe	
http://ns.ado/Ident	0%	Avira URL Cloud	safe	
http://iptc.tc4xmp	0%	Avira URL Cloud	safe	

Domains and IPs

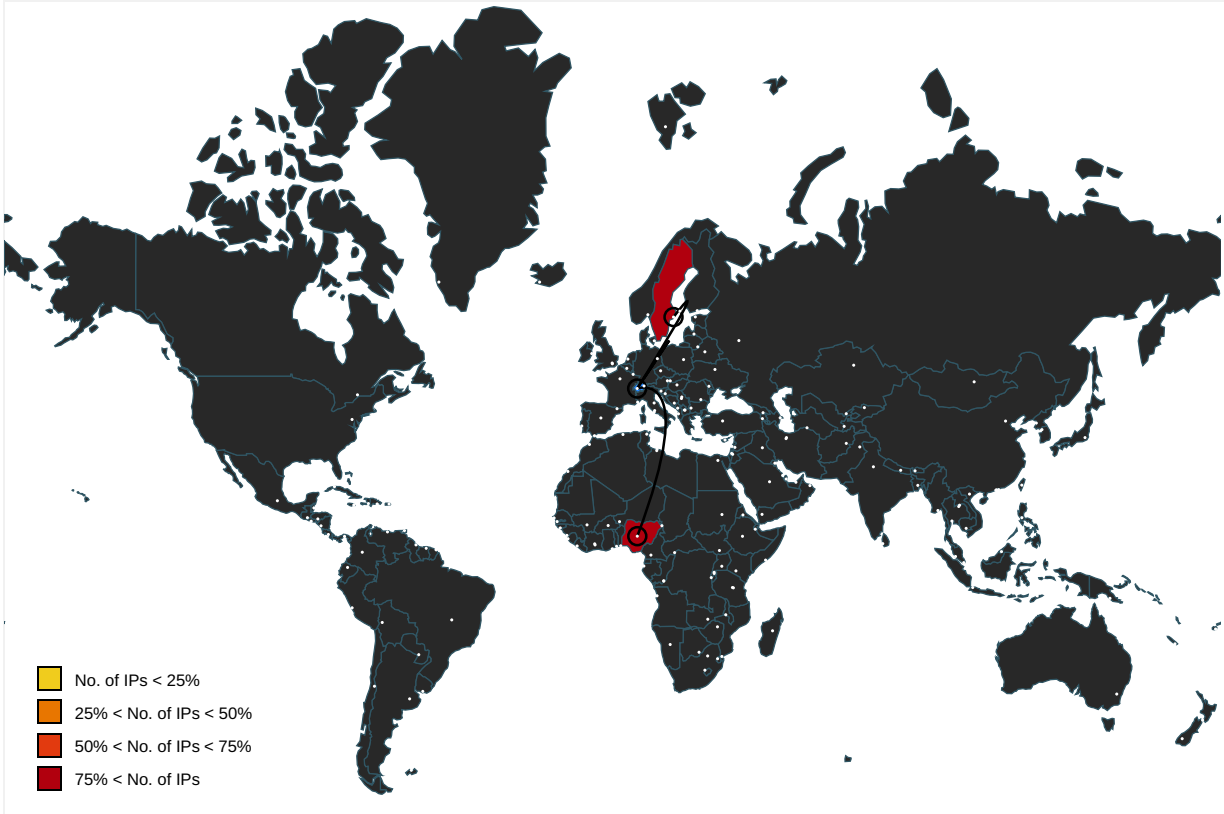
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
annapro.linkpc.net	105.112.113.90	true	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://iptc.tc4xmp:	DHL_file 187652345643476245.exe, 00000000.00000002.307699321.0000000001519000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://ns.ado/Ident	demiusda.exe, 0000000C.00000002.615285551.0000000001799000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.tc4xmp	demiusda.exe, 0000000C.00000002.615285551.0000000001799000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.157.160.233	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true
105.112.113.90	unknown	Nigeria		36873	VNL1-ASNG	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	336532
Start date:	06.01.2021
Start time:	09:25:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DHL_file 187652345643476245.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:	40
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@38/25@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 3.1% (good quality ratio 2.5%) • Quality average: 68.3% • Quality standard deviation: 32.5%
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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.42.151.234, 104.79.90.110, 104.43.193.48, 2.20.142.210, 2.20.142.209, 51.11.168.160, 52.147.198.201, 92.122.213.247, 92.122.213.194, 20.54.26.129, 168.61.161.212, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, 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, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many 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
09:26:08	API Interceptor	214x Sleep call for process: DHL_file 18765234564347624 5.exe modified
09:26:11	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\demiusda.lnk
09:26:56	API Interceptor	182x Sleep call for process: demiusda.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.157.160.233	DHL_file 18765234564347624 5.exe	Get hash	malicious	Browse	
	DHL_file 18765234564347624 5.exe	Get hash	malicious	Browse	
	DHL_file 18765234564347624 5.exe	Get hash	malicious	Browse	
	DHL_file 18765234564347624 5.exe	Get hash	malicious	Browse	
	DHL_file 18765234564347624 5.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	
	URGENT QUOTATION 473833057.exe	Get hash	malicious	Browse	
	P-O Doc #662020094753525765 3.exe	Get hash	malicious	Browse	
105.112.113.90	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
annapro.linkpc.net	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_document11022020680908911.exe	Get hash	malicious	Browse	• 129.205.11 3.251
	DHL ShipmentDHL Shipment 237590.pdf.exe	Get hash	malicious	Browse	• 129.205.12 4.172
	Doc_AWB#5305323204643_UPS.pdf.exe	Get hash	malicious	Browse	• 129.205.12 4.152

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OBE-EUROPEObenetworkEuropeSE	dpR3o92MH1.exe	Get hash	malicious	Browse	• 185.157.162.81
	0qNSJXB8nG.exe	Get hash	malicious	Browse	• 185.157.162.81
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	• 185.157.161.86
	7w7LwD8bqe.exe	Get hash	malicious	Browse	• 185.157.162.81
	ZZB5zuv1X0.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	ptoovvKZ80.exe	Get hash	malicious	Browse	• 185.157.162.81
	spetsifikatsiya.xls	Get hash	malicious	Browse	• 185.157.162.81
	EnJsj6nuD4.exe	Get hash	malicious	Browse	• 185.157.162.81
	AdviceSlip.xls	Get hash	malicious	Browse	• 217.64.149.169
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.16 0.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.16 0.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.16 0.233
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.16 0.233
	50404868-c352-422f-a608-7fd64b335eec.exe	Get hash	malicious	Browse	• 185.157.161.86
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 185.157.16 0.233
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	• 185.157.16 0.233
	URGENT QUOTATION 473833057.exe	Get hash	malicious	Browse	• 185.157.16 0.233
	P-O Doc #662020094753525765 3.exe	Get hash	malicious	Browse	• 185.157.16 0.233
	SecuriteInfo.com.Trojan.DownLoader36.26524.23979.exe	Get hash	malicious	Browse	• 185.157.16 0.202
VNL1-ASNG	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	DHL_file 187652345643476245.exe	Get hash	malicious	Browse	• 105.112.113.90
	Confirmation Copy RefNo-MT102.exe	Get hash	malicious	Browse	• 105.112.102.57
	FedExs AWB#5305323204643.exe	Get hash	malicious	Browse	• 105.112.113.90
	PAYMENT COPY.exe	Get hash	malicious	Browse	• 105.112.109.37
	PO456789.exe	Get hash	malicious	Browse	• 105.112.96.12
	DHL_10177_R293_DOCUMENT.exe	Get hash	malicious	Browse	• 105.112.10 1.201
	ibgcrnNmhB.exe	Get hash	malicious	Browse	• 105.112.25.130
	purchase order.exe	Get hash	malicious	Browse	• 105.112.25.74
	packing list.xlsx.exe	Get hash	malicious	Browse	• 105.112.69.142
	9087654.exe	Get hash	malicious	Browse	• 105.112.10 1.151

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ.exe	Get hash	malicious	Browse	• 105.112.100.239
	LOI.exe	Get hash	malicious	Browse	• 105.112.100.239
	corporate-tax.exe	Get hash	malicious	Browse	• 105.112.101.84
	QUOTATION - COVID 19 PROTECTION SOLUTIONS - final.exe	Get hash	malicious	Browse	• 105.112.124.8
	BDH9YAC4aQ.exe	Get hash	malicious	Browse	• 105.112.101.125
	JBIY8HTthL.exe	Get hash	malicious	Browse	• 105.112.101.125
	late-payment.exe	Get hash	malicious	Browse	• 105.112.45.74
	Doc0_01210_72820.exe	Get hash	malicious	Browse	• 105.112.100.246

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	SWIFT77266255378434pdf.exe	Get hash	malicious	Browse	
	SWIFT998775523434pdf.exe	Get hash	malicious	Browse	
	SWIFT345343445pdf.exe	Get hash	malicious	Browse	
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	
	1FXO8fI8R3.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Razy.820883.21352.exe	Get hash	malicious	Browse	
	SWIFT09775527743pdf.exe	Get hash	malicious	Browse	
	Pi.exe	Get hash	malicious	Browse	
	PAYMENT SLIP.EXE	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.GenericKD.45131634.12155.exe	Get hash	malicious	Browse	
	iZLqZLqNgq.exe	Get hash	malicious	Browse	
	UVZxk61Vdc.exe	Get hash	malicious	Browse	
	gVrKAqVUIw.exe	Get hash	malicious	Browse	
	OBJEDNAT- SII40513967MM793333.PDF.exe	Get hash	malicious	Browse	
	Lff0xG1Nlb.exe	Get hash	malicious	Browse	
	http___auditor3.duckdns.org_ftp.exe	Get hash	malicious	Browse	
	SDJ-0488.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.BackDoor.SpyBotNET.25.26343.exe	Get hash	malicious	Browse	
	u4MLkKgbET.exe	Get hash	malicious	Browse	
	YLL6LsHHyL.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_file 187652345643476245.exe.log	
Process:	C:\Users\user\Desktop\DHL_file 187652345643476245.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1451
Entropy (8bit):	5.345862727722058
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84G1qE4j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovGm
MD5:	06F54CDBFEF62849AF5AE052722BD7B6
SHA1:	FB0250AAC2057D0B5BCE4CE130891E428F28DA05
SHA-256:	4C039B93A728B546F49C47ED8B448D40A3553CDAABB147067AEE3958133CB446
SHA-512:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895BABB
Malicious:	**true**

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_file 187652345643476245.exe.log	
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\Microsoft\CLR_v4.0_32\UsageLogs\watchprcss.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1362
Entropy (8bit):	5.343186145897752
Encrypted:	false
SSDEEP:	24:ML9E4Ks2eE4O1lEE4UVwPKDE4KhK3VZ9pKhuE4IWUAE4KI6no84j:MxHKXeHKlEHU0YHKhQnouHIW7HKjovj
MD5:	1249251E90A1C28AB8F7235F30056DEB
SHA1:	166BA6B64E9B0D9BA7B856334F7D7EC027030BA1
SHA-256:	B5D65BF3581136CD5368BC47FA3972E06F526EED407BC6571D11D9CD4B5C4D83
SHA-512:	FD880C5B12B22241F67139ABD09B99ACE7A4DD24635FC6B340A3E7C463E2AEF3FA68EF647352132934BC1F8CA134F46064049449ACB67954BEDDEA9AA967088
Malicious:	false
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\AddInProcess32.exe	
Process:	C:\Users\user\Desktop\DHL_file 187652345643476245.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	42080
Entropy (8bit):	6.2125074198825105
Encrypted:	false
SSDEEP:	384:gc3JOvwWj8Gpw0A67dOpRIMKJ9Yl6dnPU3SERztmbqCJstdMardz/JikPZ+QsPZw:g4JU8g17dl6Iq88MoBd7mFViqM5sL2
MD5:	F2A47587431C466535F3C3D3427724BE
SHA1:	90DF719241CE04828F0DD4D31D683F84790515FF
SHA-256:	23F4A2CCDCE499C524CF43793FDA8E773D809514B5471C02FA5E68F0CDA7A10B
SHA-512:	E9D0819478DDDA47763C7F5F617CD258D0FACBBBFFE0C7A965EDE9D0D884A6D7BB445820A3FD498B243BBD8BECBA146687B61421745E32B86272232C6F9E90D8
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: SWIFT772662553784 34pdf.exe, Detection: malicious, Browse • Filename: SWIFT998775523434pdf.exe, Detection: malicious, Browse • Filename: SWIFT345343445pdf.exe, Detection: malicious, Browse • Filename: Order_1101201918_AUTECH.exe, Detection: malicious, Browse • Filename: 1FXO8fI8R3.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Razy.820883.21352.exe, Detection: malicious, Browse • Filename: SWIFT09775527743pdf.exe, Detection: malicious, Browse • Filename: Pi.exe, Detection: malicious, Browse • Filename: PAYMENT SLIP.EXE, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.GenericKD.45131634.12155.exe, Detection: malicious, Browse • Filename: iZLqZLqNgq.exe, Detection: malicious, Browse • Filename: UVZxk61Vdc.exe, Detection: malicious, Browse • Filename: gVrKAqVUIw.exe, Detection: malicious, Browse • Filename: OBJEDNAT- SII40513967MM793333.PDF.exe, Detection: malicious, Browse • Filename: Lff0xG1Nlb.exe, Detection: malicious, Browse • Filename: http___auditor3.duckdns.org_ftp.exe, Detection: malicious, Browse • Filename: SDJ-0488.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.BackDoor.SpyBotNET.25.26343.exe, Detection: malicious, Browse • Filename: u4MLkKgbET.exe, Detection: malicious, Browse • Filename: YLL6LsHHyL.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....0..X.....w... .....@.. ..... .`.....Hw..O..... .....f..`>.....v..... ....H.....text....W... ...X..... ..`.rsrc... .....Z.....@..@.relo c.....d.....@..B.....\|w.....H.....#...Q.....u.....0..K.....-..*..i....*...r...p.o....,...r...p.o....-..*.....o.....o.....$...*.....o....(....(.....:...(....o.....r...p.o.....4.....o..... .....o.....s .....o!...s".....s#.....r]..prg..po$.....r...p.o$.....r...pr...po$.....s.....(%.....tB...r...p(&...&..r...p.('...s(.....o)...&..o*....(+...o,.....&...(- ....*.....3..@.....R...s.....s....(....*:.(/.....}P...*J.{P....o0..

C:\Users\user\AppData\Local\Temp\watchprcss.exe	
Process:	C:\Users\user\AppData\Roaming\demiusda.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	78336
Entropy (8bit):	4.369296705546591
Encrypted:	false
SSDEEP:	768:jlU4+MS3Fu0thSOV4GM0SuHk9Oh/1TRIWUk7NlfaNV9KQLxXXSv:l6o03IGMLuHk+Ck5lfaNP7xSv
MD5:	0E362E7005823D0BEC3719B902ED6D62
SHA1:	590D860B909804349E0CDC2F1662B37BD62F7463
SHA-256:	2D0DC6216F613AC7551A7E70A798C22AEE8EB9819428B1357E2B8C73BEF905AD
SHA-512:	518991B68496B3F8545E418CF9B345E0791E09CC20D177B8AA47E0ABA447AA55383C64F5BDACA39F2B061A5D08C16F2AD484AF8A9F238CA23AB081618FBA3AD3
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Y .....P..&.....D... .....@.. ....`.....D..W....`.....hD..... ....H.....text...$... ...&..... ..`.rsrc.....`.....(.....@..@.rel oc.....0.....@..B.....D.....H.....l....%.....).....0..6.....(8...t....&.(8...t....&.....(8...t.....8;....8%.....(8...t....&.(8...t..... .:.....(8...t....:.....(8...t....:.....(8...t.....\:@....(8...t....&.)...&8.....(8...t....&(8...t....&.....:.....8x.....:L...88....(8...t....&(8...t....&(8...t....&(8...t.....:....8!..... (8...t....&.....(8...t....&.....(8...t....:8.....(8...t....&.

C:\Users\user\AppData\Local\Temp\watchprcss.txt	
Process:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.705892979822154
Encrypted:	false
SSDEEP:	3:ORVVNWXp5cViEaKC5YBEL4NvHn:OzjWXp+NaZ5YBEL49H
MD5:	6D53BAE6990F1C3A4F4D9729A9F99D73
SHA1:	AE73ED5B42B48B09A728BC716F690ABDE5EFDE28
SHA-256:	CAA78D20B309DFB63A791BBEB7396CF8632C02839D432751A670EE233257665B
SHA-512:	0D326A2AE317E9CDB240334805EFF947D1689DD28E7E1F43C652F284551C49CBFC13E8CD74802CBD8F648EE19AB04AB4F20B2603B710F26CF2BBC9E5BDE1E4B6
Malicious:	false
Preview:	1240..C:\Users\user\AppData\Roaming\demiusda.exe..6216..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:THt:rt
MD5:	33EE0B6F6D13E4D20830C3D041CA8765
SHA1:	E5BF757840F0F7FD17E548BB901B03037AB1DCF8
SHA-256:	3610AFA3FFB6D11775498D942115542E0A80D0CF644D6DD6849BDD0506095165
SHA-512:	D682405326C9760E3E8FABD20BF13BBD891B517C11848B9D3DFA183B3C58EA733A1906EFDBF9182880CFA71F7FDD403BF62425CA7212AC3BA06162142FAF1D8
Malicious:	**true**
Preview:	G.Yh..H

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\demiusda.lnk	
Process:	C:\Users\user\Desktop\DHL_file 187652345643476245.exe
File Type:	MS Windows shortcut, Item id list present, Has Relative path, Has Working directory, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	3.113531320897441
Encrypted:	false
SSDEEP:	12:8wl0jsXou41w/tz0/CSLYhAOwSmIiw/k3qMJ+IiwPgTCNfBT/v4t2Y+xIBjK:8kf4eWLYhAOwJwMtowPVpd7aB
MD5:	74F0FF8019BFD75A8B5FCAFE358F46AF
SHA1:	CEE790BEE58C06B1093988D86E1162309435D362
SHA-256:	7D9DD5D1A15A1F7DD748116AA608DEC866F46CDBF2DE363EBAF16D3D66A23CF3
SHA-512:	D721D3939EA6F7DA08635B15F95F964E23A885650A66836ACEFC196430D760484007C3D20AC118996BDBA356FA70069318C3B64F81D565230983C6935EA7E4C2

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\demiusda.lnk	
Malicious:	false
Preview:	L.....F.....P.O. .:i.....+00.../C:\.....P.1.....Users.<.....U.s.e.r.s.....P.1.....user.<..... .....h.a.r.d.z.....V.1.....AppData.@.....A.p.p.D.a.t.a.....V.1.....Roaming.@.....R.o.a.m.i.n.g.....f.2..... ....demiusda.exe..J.....d.e.m.i.u.s.d.a...e.x.e.....\.....\.....\.....\.....\.....\.d.e.m.i.u.s.d.a...e.x.e.+.C.:.\.U.s.e.r.s.\.h.a.r.d.z.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g .\.d.e.m.i.u.s.d.a...e.x.e.....y.....>.e.L.:..er.=y.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.- .1.0.0.2.....

C:\Users\user\AppData\Roaming\demiusda.exe	
Process:	C:\Users\user\Desktop\DHL_file 187652345643476245.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	668672
Entropy (8bit):	5.143006502161217
Encrypted:	false
SSDEEP:	6144:plckliODxvkrhDdyquS7xY+R/3HMCX7ehD4Yym6D3V2i7LkuotFN5:p+kliXIqh7x7R/XMKqxvyfFI
MD5:	303E92008EA45ABDE4FC35D8D176015D
SHA1:	29FF646C7C04A2BE614BDBE87F73DF87ADD78DDA
SHA-256:	C4DBEC4C0DF381CEE21C2BA0D6105B0F7310C8F108E66E078DF0AD4803148FB6
SHA-512:	70996F3C23154F43E7F6443FCEDCF54372660C19FFB57689380450B46C9DBA3AF18B50569380AECB5B3D52C705DC16E48B165F2ECE179BA8671191C5E01EC1C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 23%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....pEC.....(.....G... ...`....@.. ..... ..`.....G..O....`..... ..... ..H.....text....'... ...(..... ..`.rsrc.....`.....*.....@..@.reloc..... .....2.....@..B.....G.....H.....$..."......9.....5.....0.!.dW....U.B{..|..7{f.X.Ye...ri..*.W!dd.K.e....q{..q{.R...Yj..OU#...[.Z.0.rq..ht_1.....XP..... U..=...tp.....\MX.]....O..`..\.....ek.<Z.pO.n3_...2.....8....d.{.6i...gXCE.z.....Z+....t...=.....(.c.N..C...4_...SP#...e.B].....q..]s.....E?...jfv[.4.....:...e.W.D.sD.....Yq...J..... 5.... ..#.....L.....;.....U...<...F8.....*..,S.....rj.....\)..`....p..

C:\Users\user\AppData\Roaming\demiusda.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DHL_file 187652345643476245.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**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.143006502161217
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_file 187652345643476245.exe
File size:	668672
MD5:	303e92008ea45abde4fc35d8d176015d
SHA1:	29ff646c7c04a2be614bdbe87f73df87add78dda
SHA256:	c4dbec4c0df381cee21c2ba0d6105b0f7310c8f108e66e078df0ad4803148fb6

General

SHA512:	70996f3c23154f43e7f6443fcedcf54372660c19ffb57689380450b46c9dba3af18b50569380aecb5b3d52c705dc16e48b165f2ece179ba8671191c5e01ec1cd
SSDEEP:	6144:plckliODxvkrhDdyquS7xY+R/3HMCX7ehD4Yym6D3V2i7LkuotFN5:p+kliXIqh7x7R/XMKqxvyfFI
File Content Preview:	MZ......................@..!..L.!This program cannot be run in DOS mode....$.......PE..L....pEC.................(...........G... ...`....@.. ................................`.................................

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a47ee
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:	0x4345708B [Thu Oct 6 18:44:27 2005 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xa479c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa6000	0x60a	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa8000	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	0xa27f4	0xa2800	False	0.505387620192	data	5.14906503317	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa6000	0x60a	0x800	False	0.3427734375	data	3.60047757985	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa8000	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_VERSION	0xa60a0	0x380	data		
RT_MANIFEST	0xa6420	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

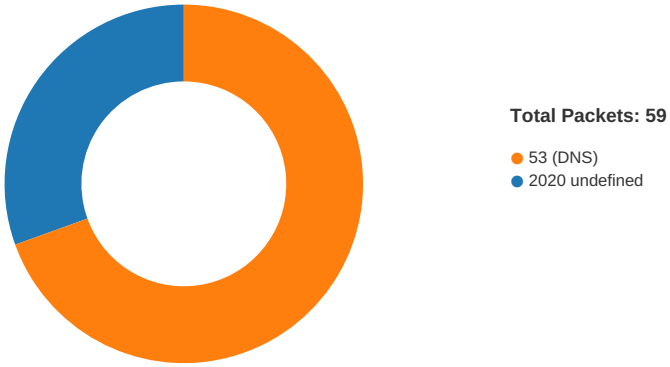
Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 1995 :F7C@?H6B:@5A>3@
Assembly Version	1.0.0.0
InternalName	emekaike.exe
FileVersion	2.3.4.5
CompanyName	:F7C@?H6B:@5A>3@
Comments	FB;I;IG>C=B?C9:7
ProductName	3F;D9H8B;FJ77<J=5G=3
ProductVersion	2.3.4.5

Description	Data
FileDescription	3F;D9H8B;FJ77<J=5G=3
OriginalFilename	emekaike.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 09:27:33.786709070 CET	49724	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:27:36.895843983 CET	49724	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:27:42.911953926 CET	49724	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:27:52.137356997 CET	49731	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:27:55.140928984 CET	49731	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:28:01.147874117 CET	49731	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:28:09.603240013 CET	49736	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:28:12.664458990 CET	49736	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:28:18.665035009 CET	49736	2020	192.168.2.3	185.157.160.233
Jan 6, 2021 09:28:28.262279034 CET	49744	2020	192.168.2.3	105.112.113.90
Jan 6, 2021 09:28:31.369132996 CET	49744	2020	192.168.2.3	105.112.113.90
Jan 6, 2021 09:28:37.369640112 CET	49744	2020	192.168.2.3	105.112.113.90
Jan 6, 2021 09:28:47.495038986 CET	49745	2020	192.168.2.3	105.112.113.90
Jan 6, 2021 09:28:50.636318922 CET	49745	2020	192.168.2.3	105.112.113.90
Jan 6, 2021 09:28:56.732465982 CET	49745	2020	192.168.2.3	105.112.113.90
Jan 6, 2021 09:29:07.716557026 CET	49756	2020	192.168.2.3	105.112.113.90
Jan 6, 2021 09:29:10.729454994 CET	49756	2020	192.168.2.3	105.112.113.90
Jan 6, 2021 09:29:16.729943991 CET	49756	2020	192.168.2.3	105.112.113.90

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 09:26:07.494633913 CET	50620	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:07.542588949 CET	53	50620	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:08.740783930 CET	64938	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:08.788851976 CET	53	64938	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:10.001523018 CET	60152	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:10.049612045 CET	53	60152	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:14.027250051 CET	57544	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:14.075248957 CET	53	57544	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:16.293397903 CET	55984	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:16.352514982 CET	53	55984	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:30.863061905 CET	64185	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:30.922390938 CET	53	64185	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 09:26:41.786823988 CET	65110	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:41.843266964 CET	53	65110	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:44.343044043 CET	58361	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:44.391012907 CET	53	58361	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:46.261770010 CET	63492	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:46.320998907 CET	53	63492	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:48.241674900 CET	60831	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:48.597884893 CET	53	60831	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:49.298086882 CET	60100	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:49.348786116 CET	53	60100	8.8.8.8	192.168.2.3
Jan 6, 2021 09:26:59.944364071 CET	53195	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:26:59.992388010 CET	53	53195	8.8.8.8	192.168.2.3
Jan 6, 2021 09:27:02.138602018 CET	50141	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:27:02.197505951 CET	53	50141	8.8.8.8	192.168.2.3
Jan 6, 2021 09:27:18.218920946 CET	53023	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:27:18.282691002 CET	53	53023	8.8.8.8	192.168.2.3
Jan 6, 2021 09:27:27.543916941 CET	49563	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:27:27.594078064 CET	53	49563	8.8.8.8	192.168.2.3
Jan 6, 2021 09:27:35.379808903 CET	51352	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:27:35.436439037 CET	53	51352	8.8.8.8	192.168.2.3
Jan 6, 2021 09:27:36.046333075 CET	59349	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:27:36.094225883 CET	53	59349	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:03.951165915 CET	57084	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:03.998981953 CET	53	57084	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:08.051258087 CET	58823	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:08.099241972 CET	53	58823	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:09.367156029 CET	57568	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:09.415255070 CET	50540	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:09.415271044 CET	53	57568	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:09.489496946 CET	53	50540	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:12.442214012 CET	54366	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:12.490132093 CET	53	54366	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:13.524734974 CET	53034	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:13.572575092 CET	53	53034	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:14.642323971 CET	57762	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:14.690243006 CET	53	57762	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:16.154258013 CET	55435	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:16.210279942 CET	53	55435	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:17.323147058 CET	50713	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:17.378025055 CET	53	50713	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:18.371445894 CET	56132	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:18.422231913 CET	53	56132	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:19.351128101 CET	58987	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:19.398963928 CET	53	58987	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:28.048451900 CET	56579	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:28.209052086 CET	53	56579	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:47.425271988 CET	60633	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:47.481437922 CET	53	60633	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:52.147876024 CET	61292	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:52.204247952 CET	53	61292	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:52.717561007 CET	63619	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:52.773730993 CET	53	63619	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:53.292967081 CET	64938	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:53.349289894 CET	53	64938	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:54.042546988 CET	61946	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:54.109565973 CET	53	61946	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:54.566910982 CET	64910	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:54.623078108 CET	53	64910	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:55.138413906 CET	52123	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:55.197541952 CET	53	52123	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:55.695528984 CET	56130	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:55.754605055 CET	53	56130	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:56.330974102 CET	56338	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:56.378962040 CET	53	56338	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 6, 2021 09:28:57.080907106 CET	59420	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:57.137142897 CET	53	59420	8.8.8.8	192.168.2.3
Jan 6, 2021 09:28:57.533690929 CET	58784	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:28:57.589957952 CET	53	58784	8.8.8.8	192.168.2.3
Jan 6, 2021 09:29:07.639687061 CET	63978	53	192.168.2.3	8.8.8.8
Jan 6, 2021 09:29:07.695921898 CET	53	63978	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 6, 2021 09:28:28.048451900 CET	192.168.2.3	8.8.8.8	0xb75c	Standard query (0)	annapro.linkpc.net	A (IP address)	IN (0x0001)
Jan 6, 2021 09:28:47.425271988 CET	192.168.2.3	8.8.8.8	0x3a5c	Standard query (0)	annapro.linkpc.net	A (IP address)	IN (0x0001)
Jan 6, 2021 09:29:07.639687061 CET	192.168.2.3	8.8.8.8	0x63c	Standard query (0)	annapro.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 6, 2021 09:28:28.209052086 CET	8.8.8.8	192.168.2.3	0xb75c	No error (0)	annapro.linkpc.net		105.112.113.90	A (IP address)	IN (0x0001)
Jan 6, 2021 09:28:47.481437922 CET	8.8.8.8	192.168.2.3	0x3a5c	No error (0)	annapro.linkpc.net		105.112.113.90	A (IP address)	IN (0x0001)
Jan 6, 2021 09:29:07.695921898 CET	8.8.8.8	192.168.2.3	0x63c	No error (0)	annapro.linkpc.net		105.112.113.90	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

- DHL_file 187652345643476245.exe
- demiusda.exe
- AddInProcess32.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe
- watchprcss.exe

Click to jump to process

System Behavior

Analysis Process: DHL_file 187652345643476245.exe PID: 6652 Parent PID: 5636

General

Start time:	09:26:04
Start date:	06/01/2021
Path:	C:\Users\user\Desktop\DHL_file 187652345643476245.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DHL_file 187652345643476245.exe'
Imagebase:	0xbc0000
File size:	668672 bytes
MD5 hash:	303E92008EA45ABDE4FC35D8D176015D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	6DBDCF06	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	6DBDCF06	unknown
C:\Users\user\AppData\Local\Temp\AddInProcess32.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	57ACE43	CopyFileExW
C:\Users\user\AppData\Roaming\demiusda.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	57ACE43	CopyFileExW
C:\Users\user\AppData\Roaming\demiusda.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	57ACE43	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_file 187652345643476245.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEEC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	0	42080	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 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 1d 5a 8e 5a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 58 00 00 00 0c 00 00 00 00 00 00 9a 77 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 dc 8d 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..X...........w... ....@.. ....`.................	success or wait	1	57ACE43	CopyFileExW
C:\Users\user\AppData\Roaming\demiusda.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 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 8b 70 45 43 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 28 0a 00 00 0a 00 00 00 00 00 00 ee 47 0a 00 00 20 00 00 00 60 0a 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 a0 0a 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....pEC.......... ....(...........G... ...`....@.. ........................ ............`.................	success or wait	3	57ACE43	CopyFileExW
C:\Users\user\AppData\Roaming\demiusda.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	57ACE43	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DHL_file18765234564347624 5.exe.log	unknown	1451	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 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	6DEEC907	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	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBB5705	unknown

Analysis Process: demiusda.exe PID: 1240 Parent PID: 6652

General

Start time:	09:26:49
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Roaming\demiusda.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\demiusda.exe'
Imagebase:	0xd50000
File size:	668672 bytes

MD5 hash:	303E92008EA45ABDE4FC35D8D176015D
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: 0000000C.00000002.623749902.0000000004231000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.623749902.0000000004231000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.623749902.0000000004231000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.624626944.0000000004DB7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.624626944.0000000004DB7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.624626944.0000000004DB7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000C.00000002.624416649.0000000004CEA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.624416649.0000000004CEA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.624416649.0000000004CEA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 23%, 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	6DBDCF06	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	6DBDCF06	unknown
C:\Users\user\AppData\Local\Temp\watchprcss.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW
C:\Users\user\AppData\Local\Temp\watchprcss.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CB21E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	54	31 32 34 30 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 64 65 6d 69 75 73 64 61 2e 65 78 65 0d 0a 30 0d 0a	1240..C:\Users\user\AppData\Roaming\demiusda.exe..0..	success or wait	1	6CB21B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\watchprcss.exe	unknown	78336	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 59 20 14 c7 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 26 01 00 00 0a 00 00 00 00 00 00 de 44 01 00 00 20 00 00 00 00 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 a0 01 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 00 10 00 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode....$.......PE..L...Y ....P..&...........D... ....@.. ....`................	success or wait	1	6CB21B4F	WriteFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	54	31 32 34 30 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 64 65 6d 69 75 73 64 61 2e 65 78 65 0d 0a 30 0d 0a	1240..C:\Users\user\AppData\Roaming\demiusda.exe..0..	success or wait	8	6CB21B4F	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	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBB5705	unknown
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	8	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	8	6CB21B4F	ReadFile

Analysis Process: AddInProcess32.exe PID: 1256 Parent PID: 1240

General

Start time:	09:27:26
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\AddInProcess32.exe
Imagebase:	0x7ff7488e0000
File size:	42080 bytes
MD5 hash:	F2A47587431C466535F3C3D3427724BE
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: 00000011.00000002.624186822.0000000005610000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000011.00000002.624186822.0000000005610000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.620217311.0000000003F19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.620217311.0000000003F19000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.624595498.0000000005A80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000011.00000002.624595498.0000000005A80000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.624595498.0000000005A80000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.615389852.0000000002ED1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.607848743.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.607848743.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.607848743.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 0%, Virustotal, Browse • 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	6DBDCF06	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	6DBDCF06	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	6CB2BEFF	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	6CB21E60	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	6CB2BEFF	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	6CB2BEFF	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	47 d6 be 59 68 b2 d8 48	G..Yh..H	success or wait	1	6CB21B4F	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	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	unknown	4096	success or wait	1	6DB9D72F	unknown
C:\Users\user\AppData\Local\Temp\AddInProcess32.exe	unknown	512	success or wait	1	6DB9D72F	unknown

Analysis Process: watchprcss.exe PID: 5164 Parent PID: 1240

General

Start time:	09:27:36
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xe20000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\watchprcss.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DEEC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	57	31 32 34 30 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 64 65 6d 69 75 73 64 61 2e 65 78 65 0d 0a 35 31 36 34 0d 0a	1240..C:\Users\user\AppData\Roaming\demiusda.exe..5164..	success or wait	1	6CB21B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\watchprcss.exe.log	unknown	1362	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 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	6DEEC907	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	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DB103DE	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile

Analysis Process: watchprcss.exe PID: 6304 Parent PID: 5164

General

Start time:	09:27:38
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0x200000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	57	31 32 34 30 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 64 65 6d 69 75 73 64 61 2e 65 78 65 0d 0a 36 33 30 34 0d 0a	1240..C:\Users\user\AppData\Roaming\demiusda.exe..6304..	success or wait	1	6CB21B4F	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	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DB103DE	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile

Analysis Process: watchprcss.exe PID: 5712 Parent PID: 1240

General

Start time:	09:27:43
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xe40000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	57	31 32 34 30 0d 0a 43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 64 65 6d 69 75 73 64 61 2e 65 78 65 0d 0a 35 37 31 32 0d 0a	1240..C:\Users\user\AppData\Roaming\demiusda.exe..5712..	success or wait	1	6CB21B4F	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	6DBB5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DBB5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DB103DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DBBCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DB103DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6DB103DE	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile
C:\Users\user\AppData\Local\Temp\watchprcss.txt	unknown	4096	success or wait	1	6CB21B4F	ReadFile

Analysis Process: watchprcss.exe PID: 5404 Parent PID: 5712

General

Start time:	09:27:45
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'

Imagebase:	0xee0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: watchprcss.exe PID: 6660 Parent PID: 1240

General

Start time:	09:27:50
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0x940000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: watchprcss.exe PID: 5024 Parent PID: 6660

General

Start time:	09:27:54
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xf30000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: watchprcss.exe PID: 4076 Parent PID: 1240

General

Start time:	09:27:57
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xa80000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: watchprcss.exe PID: 6508 Parent PID: 4076

General

Start time:	09:28:00
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0x4f0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: watchprcss.exe PID: 7020 Parent PID: 1240

General

Start time:	09:28:03
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xdd0000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: watchprcss.exe PID: 476 Parent PID: 7020

General

Start time:	09:28:06
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0x410000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: watchprcss.exe PID: 6284 Parent PID: 1240

General

Start time:	09:28:10
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xf10000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

Analysis Process: watchprcss.exe PID: 1724 Parent PID: 6284

General

Start time:	09:28:16
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xd40000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: watchprcss.exe PID: 7040 Parent PID: 1240

General

Start time:	09:28:21
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0x90000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: watchprcss.exe PID: 3032 Parent PID: 7040

General

Start time:	09:28:24
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xa80000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true

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

Analysis Process: watchprcss.exe PID: 7000 Parent PID: 1240

General

Start time:	09:28:29
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0xc30000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: watchprcss.exe PID: 6216 Parent PID: 7000

General

Start time:	09:28:35
Start date:	06/01/2021
Path:	C:\Users\user\AppData\Local\Temp\watchprcss.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\watchprcss.exe'
Imagebase:	0x990000
File size:	78336 bytes
MD5 hash:	0E362E7005823D0BEC3719B902ED6D62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Disassembly

Code Analysis