ID: 339185
Sample Name: DINTEC PO.exe
Cookbook: default.jbs
Time: 16:59:35
Date: 13/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

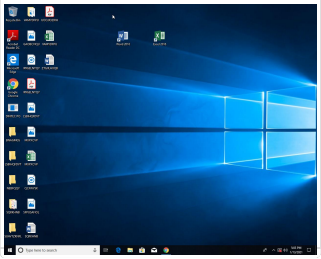
Analysis Report DINTEC PO.exe

Overview

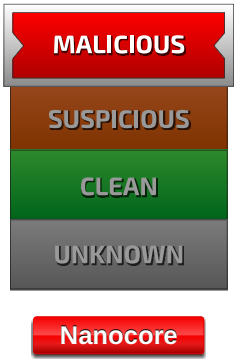
General Information

Sample Name:	DINTEC PO.exe
Analysis ID:	339185
MD5:	f1d00b68162820d.
SHA1:	406621cc2e30d1..
SHA256:	29800b7d8e8c3c..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection

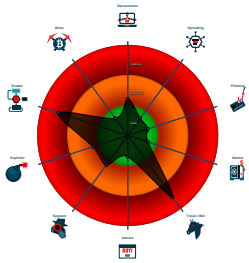


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- Allocates memory in foreign process…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Uses dynamic DNS services
- Writes to foreign memory regions
- Checks if Antivirus/Antispyware/Fire…
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- DINTEC PO.exe (PID: 4584 cmdline: 'C:\Users\user\Desktop\DINTEC PO.exe' MD5: F1D00B68162820D29EB884A91B9E6A09)
  - a.exe (PID: 6040 cmdline: 'C:\Users\user\AppData\Roaming\a.exe' MD5: F1D00B68162820D29EB884A91B9E6A09)
- a.exe (PID: 6896 cmdline: 'C:\Users\user\AppData\Roaming\a.exe' MD5: F1D00B68162820D29EB884A91B9E6A09)
  - InstallUtil.exe (PID: 6676 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- dhcpmon.exe (PID: 4904 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: EFEC8C379D165E3F33B536739AEE26A3)
  - conhost.exe (PID: 6128 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
00000004.00000003.901015469.000000000483 8000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x20f2:$a: NanoCore • 0x2117:$a: NanoCore • 0x2170:$a: NanoCore • 0x1230d:$a: NanoCore • 0x12333:$a: NanoCore • 0x1238f:$a: NanoCore • 0x1f1e4:$a: NanoCore • 0x1f23d:$a: NanoCore • 0x1f270:$a: NanoCore • 0x1f49c:$a: NanoCore • 0x1f518:$a: NanoCore • 0x1fb31:$a: NanoCore • 0x1fc7a:$a: NanoCore • 0x2014e:$a: NanoCore • 0x20435:$a: NanoCore • 0x2044c:$a: NanoCore • 0x259ea:$a: NanoCore • 0x25a64:$a: NanoCore • 0x2a601:$a: NanoCore • 0x2b9bb:$a: NanoCore • 0x2ba05:$a: NanoCore
00000002.00000002.1055562426.00000000041 EF000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10ef7:$x1: NanoCore.ClientPluginHost • 0x43aa5:$x1: NanoCore.ClientPluginHost • 0x10f34:$x2: IClientNetworkHost • 0x43ae2:$x2: IClientNetworkHost • 0x14a67:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x47615:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000002.00000002.1055562426.00000000041 EF000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000002.00000002.1055562426.00000000041 EF000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x10c5f:$a: NanoCore • 0x10c6f:$a: NanoCore • 0x10ea3:$a: NanoCore • 0x10eb7:$a: NanoCore • 0x10ef7:$a: NanoCore • 0x4380d:$a: NanoCore • 0x4381d:$a: NanoCore • 0x43a51:$a: NanoCore • 0x43a65:$a: NanoCore • 0x43aa5:$a: NanoCore • 0x10cbe:$b: ClientPlugin • 0x10ec0:$b: ClientPlugin • 0x10f00:$b: ClientPlugin • 0x4386c:$b: ClientPlugin • 0x43a6e:$b: ClientPlugin • 0x43aae:$b: ClientPlugin • 0x10de5:$c: ProjectData • 0x43993:$c: ProjectData • 0x117ec:$d: DESCrypto • 0x4439a:$d: DESCrypto • 0x191b8:$e: KeepAlive
00000000.00000002.717848221.00000000049A F000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x10ef7:$x1: NanoCore.ClientPluginHost • 0x43aa5:$x1: NanoCore.ClientPluginHost • 0x10f34:$x2: IClientNetworkHost • 0x43ae2:$x2: IClientNetworkHost • 0x14a67:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x47615:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 19 entries				

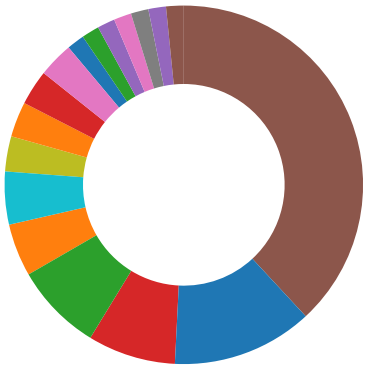
Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview

- AV Detection
- Compliance
- Software Vulnerabilities



- Networking
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Yara detected Nanocore RAT

Networking:

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

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:

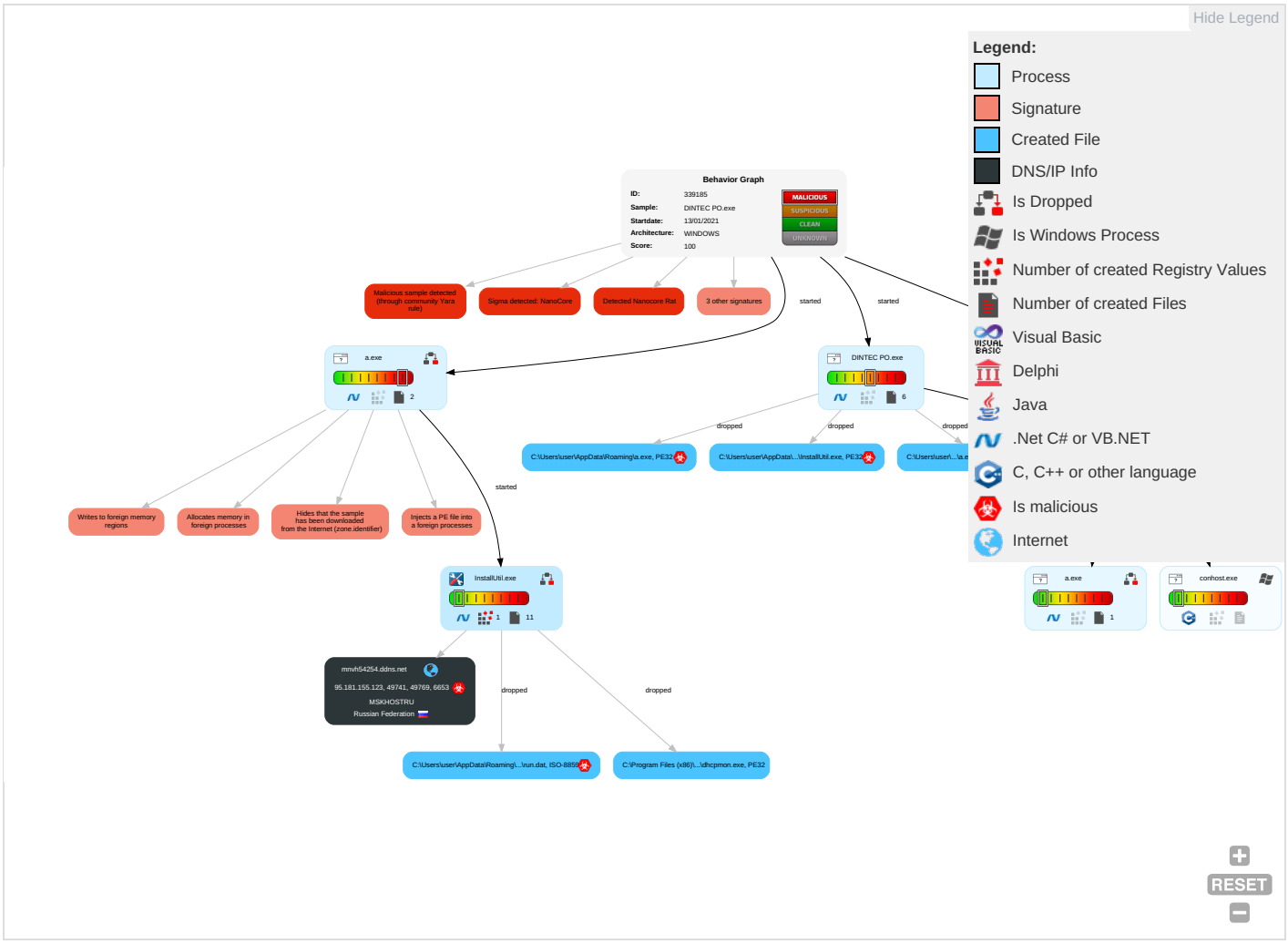
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts 1	Windows Management Instrumentation 1	Startup Items 1	Startup Items 1	Masquerading 2	OS Credential Dumping	Query Registry 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Inse Netw Com
Default Accounts	Scheduled Task/Job	Valid Accounts 1	Valid Accounts 1	Valid Accounts 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Expl Redi Calls
Domain Accounts	At (Linux)	Registry Run Keys / Startup Folder 2	Access Token Manipulation 1	Access Token Manipulation 1	Security Account Manager	Virtualization/Sandbox Evasion 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Expl Trac Loca
Local Accounts	At (Windows)	DLL Side-Loading 1	Process Injection 3 1 2	Virtualization/Sandbox Evasion 3	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2	Disable or Modify Tools 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	DLL Side-Loading 1	Process Injection 3 1 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Serv
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dow Inse Prot
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mnvh54254.ddns.net	4%	Virustotal		Browse

URLs

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

Domains and IPs

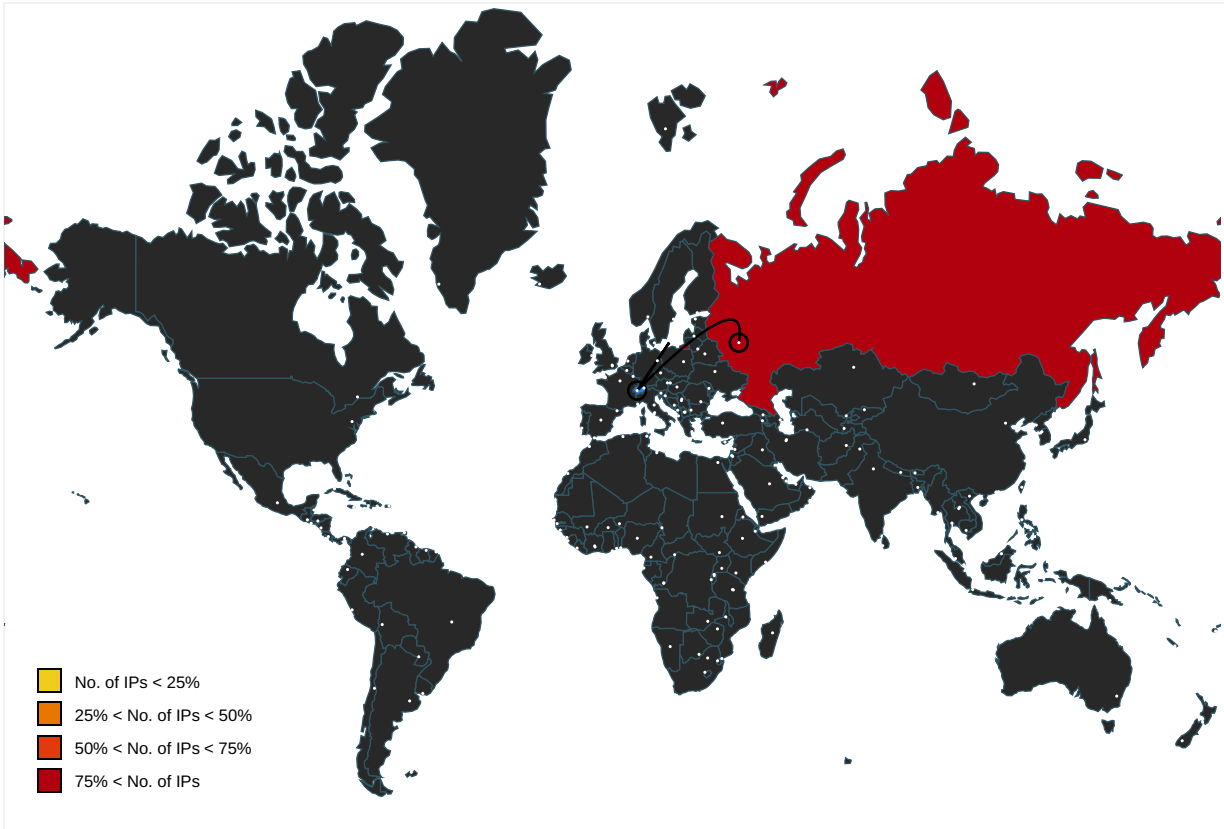
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mnvh54254.ddns.net	95.181.155.123	true	true	• 4%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ns.ado/Ident	DINTEC PO.exe, 00000000.00000003.714561873.0000000001729000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://iptc.tc4xmp	DINTEC PO.exe, 00000000.00000003.714561873.0000000001729000.00000004.00000001.sdmp, a.exe, 00000002.00000002.1048821973.0000000000BD9000.00000004.00000040.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
95.181.155.123	unknown	Russian Federation		207319	MSKHOSTRU	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339185
Start date:	13.01.2021
Start time:	16:59:35
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	DINTEC PO.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:	21
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@8/13@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.3%) • Quality average: 60.4% • Quality standard deviation: 32.6%
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. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.193.48, 51.11.168.160, 52.147.198.201, 92.122.213.247, 92.122.213.194, 2.20.142.209, 2.20.142.210, 52.155.217.156, 20.54.26.129, 93.184.220.29 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, cs9.wac.phicdn.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, skypedataprdcolcus15.cloudapp.net, skypedataprdcoleus16.cloudapp.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, blobcollector.events.data.trafficmanager.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, crl3.digicert.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:00:38	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk
17:01:01	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MSKHOSTRU	MPnIQlfxon.exe	Get hash	malicious	Browse	• 95.181.157.160

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	tyoO13LUym.exe	Get hash	malicious	Browse	• 95.181.157.160
	LutcV95NdW.exe	Get hash	malicious	Browse	• 95.181.152.100
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 95.181.157.160
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 95.181.157.160
	SecuriteInfo.com.BehavesLike.Win32.Trojan.jc.exe	Get hash	malicious	Browse	• 95.181.157.160
	pSFEOooHmL.exe	Get hash	malicious	Browse	• 95.181.152.177
	q1ClS5bciI.exe	Get hash	malicious	Browse	• 95.181.152.100
	9xeZGfuoV5.exe	Get hash	malicious	Browse	• 95.181.152.177
	L7SzoVpjhW.exe	Get hash	malicious	Browse	• 95.181.152.177
	FIq05ylmFa.exe	Get hash	malicious	Browse	• 95.181.152.100
	noo8xFTpNS.exe	Get hash	malicious	Browse	• 95.181.152.177
	YWkOcHQwEy.exe	Get hash	malicious	Browse	• 95.181.152.177
	0vuI5XGGlG.exe	Get hash	malicious	Browse	• 95.181.152.177
	FMBRNIuDlj.exe	Get hash	malicious	Browse	• 95.181.152.177
	4niFjutXp6.exe	Get hash	malicious	Browse	• 95.181.152.100
	Z1Dlmc2efo.exe	Get hash	malicious	Browse	• 95.181.152.100
	voq4kj1z14.exe	Get hash	malicious	Browse	• 95.181.152.100
	3VLexOmRKM.exe	Get hash	malicious	Browse	• 95.181.152.177
	NfeMUeolmz.exe	Get hash	malicious	Browse	• 95.181.152.177

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	PO-5042.exe	Get hash	malicious	Browse	
	New Year Order 18723TW.exe	Get hash	malicious	Browse	
	PO-75013.exe	Get hash	malicious	Browse	
	MV. Double Miracle.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Generic.mg.5a4b41327cabca49.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.FileRepMalware.exe	Get hash	malicious	Browse	
	MV Double Miracle.exe	Get hash	malicious	Browse	
	TD-10057.exe	Get hash	malicious	Browse	
	Ziraat Bankasi Swift Mesaji.exe	Get hash	malicious	Browse	
	ndSscoDob9.exe	Get hash	malicious	Browse	
	DXXJmIDl3C.exe	Get hash	malicious	Browse	
	0YdVJ6vqhO.exe	Get hash	malicious	Browse	
	TT Payment Invoice.exe	Get hash	malicious	Browse	
	al9LrOC8eM.exe	Get hash	malicious	Browse	
	M4FBPQPaus.exe	Get hash	malicious	Browse	
	hcL39YT1CR.exe	Get hash	malicious	Browse	
	XaAUv98B2a.exe	Get hash	malicious	Browse	
	04XP8gXrF7.exe	Get hash	malicious	Browse	
	zosFl3kiAK.exe	Get hash	malicious	Browse	
	4G5zLURjk4.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.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

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: PO-5042.exe, Detection: malicious, Browse • Filename: New Year Order 18723TW.exe, Detection: malicious, Browse • Filename: PO-75013.exe, Detection: malicious, Browse • Filename: MV. Double Miracle.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Generic.mg.5a4b41327cabca49.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.FileRepMalware.exe, Detection: malicious, Browse • Filename: MV Double Miracle.exe, Detection: malicious, Browse • Filename: TD-10057.exe, Detection: malicious, Browse • Filename: Ziraat Bankasi Swift Mesaji.exe, Detection: malicious, Browse • Filename: ndSscoDob9.exe, Detection: malicious, Browse • Filename: DXXJmIDl3C.exe, Detection: malicious, Browse • Filename: 0YdVJ6vqhO.exe, Detection: malicious, Browse • Filename: TT Payment Invoice.exe, Detection: malicious, Browse • Filename: al9LrOC8eM.exe, Detection: malicious, Browse • Filename: M4FBPQPaus.exe, Detection: malicious, Browse • Filename: hcL39YT1CR.exe, Detection: malicious, Browse • Filename: XaAUv98B2a.exe, Detection: malicious, Browse • Filename: 04XP8gXrF7.exe, Detection: malicious, Browse • Filename: zosFl3kiAK.exe, Detection: malicious, Browse • Filename: 4G5zLURjk4.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\Local\Microsoft\CLR_v4.0_32\UsageLogs\DINTEC PO.exe.log	
Process:	C:\Users\user\Desktop\DINTEC PO.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:	34EF5F6D5EAB0E5B11AC81F0D72FC56304291EDEEF6D19DF7145FDECAB5D342767DBBC0B4384B8DECB5741E6B85A4B431DF14FBEB5DDF2DEE103064D2895E ABB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf 3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"Present ationFramework, 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\a.exe.log	
Process:	C:\Users\user\AppData\Roaming\a.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
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.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\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	950
Entropy (8bit):	5.350971482944737
Encrypted:	false
SSDEEP:	24:MLiKNE4qpE4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7a:MeIH2HKXwYHKhQnoPtHoxHhAHKzva
MD5:	CEE81B7EB08EE82CFE49E47B81B50D1A
SHA1:	4746C7068BD50E3309BFFDBE8983B8F27D834DFD
SHA-256:	B9A90255691E7C9D3CCBD27D00FC514DDD6087446D8DB03335CEF1B5634CC460
SHA-512:	AF5865439412974FCB6B11E22CFFF1ACA0BEBF83CF398D6056CEEF93720AF0FBCB579858C39E6AA0D989680F2180F2CA181D7D12887604B420D0E1976B8AEA7
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
Process:	C:\Users\user\Desktop\DINTEC PO.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:ZBMs2SqdD86lq8gZZFyViML3an
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
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\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:cPn:s
MD5:	04893A4DCE1D8CAEF2FD3842F08DB1CE
SHA1:	BD5634B7271F155892370BFF98C8A1A176B9A4B7
SHA-256:	BCD45F69F8A5CC43EBD63DC98FFFD784B812A8167151904E1A60A3D01EEFB54B
SHA-512:	36BB8589984D8407442E6EF0A659ABEF6760165015CDE7752417D2FF24FF05E228CDF28F887ED492BB51F02C7A2FCD073D29F097DCB1FD566CBEA31940EA3EC
Malicious:	**true**
Preview:	..dk..H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'..}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?,,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk	
Process:	C:\Users\user\Desktop\DINTEC PO.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):	854
Entropy (8bit):	3.0159112944533297
Encrypted:	false
SSDEEP:	12:8wl0RsXowAOcQ/tz0/CSLm9RKMJkHgTCNfBT/v4t2Y+xIBjK:8iLDWLYr+Vpd7aB
MD5:	CDE31B0A7CA104AEE6CB2FF9ABFED71F

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.lnk	
SHA1:	B92338857A61560D0E667E6E3EB5B9CCF22CE260
SHA-256:	A835B03B57A7941B592CCF6825F308CDA3158A53B4B798B0E14C51D3E9DB1AB1
SHA-512:	AF3C36C759A831D5366F2493A4AAF7BA2A97181D098C4E2D2394F06BC379A3D947A8D2BFCFDA2ADE9C3D6AC44B0895C0E4470AA8AECF1D960C7424E2E6FAE9D
Malicious:	false
Preview:	L.................F...P.O. .:i.....+00.../C:\..................P.1..........Users.<..U.s.e.r.s.....P.1..........user.<................. ....j.o.n.e.s.....V.1..........AppData.@..A.p.p.D.a.t.a.....V.1..........Roaming.@..R.o.a.m.i.n.g.....P.2....... ....a.exe.<..a...e.x.e............\.....\.....\.....\.....\.a...e.x.e.$.C.:.\.U.s.e.r.s.\.j.o.n.e.s.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.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\a.exe	
Process:	C:\Users\user\Desktop\DINTEC PO.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	862720
Entropy (8bit):	5.4197749658829855
Encrypted:	false
SSDEEP:	6144:xMpm7XDISoFhkENO4jfCbN898MyDqFNb7LWt+Ao23KB2pTwcSn9vCfEvg4J:xszDNj6u8My+b/WtI23d9ZSn9Vd
MD5:	F1D00B68162820D29EB884A91B9E6A09
SHA1:	406621CC2E30D19645513296FE1C5F50DD6C3848
SHA-256:	29800B7D8E8C3C60918A37C992A2890B4CCF9E4E0C949ACCD48821302D0F2891
SHA-512:	B9098F02C929F9A59B4ADB846B47152D8EE69261D14558B3C2BF3BAFD35AC2A81E690C02C1F5DC6F6BEF694E4F79F668FBC16A20AB747914C570ABE8F22901FE
Malicious:	**true**
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L... .,0.............P.............N<... ...@....@.. ....`.................................;..O....@......................`.. ....H............text...T.... ....`.rsrc........@....... ..............@..@.rel oc.......`.......(..............@..B................0<......H.......@....*......_...tu..&..(.....*.s.........s.........s.........s ....*&........*"........*Vs!...(3...t.........*..(4...*..(....* N. ....(5....*V....(J........(:....*^.~....(f........(=....*v.~....~.....(H........(A....*.....(V....*^......(F...t....od....*..(G...*....0..2........("...t....("...t0...(H...t1...;..................1.......-=("...t....&(". ..t............("...t0...........(H...t....&+K.("...t...............

C:\Users\user\AppData\Roaming\a.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\DINTEC PO.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

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2017
Entropy (8bit):	4.663189584482275
Encrypted:	false
SSDEEP:	48:zK4Qu4D4ql0+1AcJRy0EJP64gFljVlWo3ggxUnQK2qmBvgw1+5:zKJDEcTytNe3Wo3uQVBIe+5
MD5:	9C305D95E7DA8FCA9651F7F426BB25BC
SHA1:	FDB5C18C26CF5B83EF5DC297C0F9CEBEF6A97FFC
SHA-256:	444F71CF504D22F0EE88024D61501D3B79AE5D1AFD521E72499F325F6B0B82BE
SHA-512:	F2829518AE0F6DD35C1DE1175FC8BE3E52EDCAFAD0B2455AC593F5E5D4BD480B014F52C3AE24E742B914685513BE5DF862373E75C45BB7908C775D7E2E404D3
Malicious:	false
Preview:	Microsoft (R) .NET Framework Installation utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Usage: InstallUtil [/u | /uninstall] [option [...]] assembly [[option [...]] assembly] [...]]....InstallUtil executes the installers in each given assembly...If the /u or /uninstall switch is specified, it uninstalls..the assemblies, otherwise it installs them. Unlike other..options, /u applies to all assemblies, regardless of where it..appears on the command line.....Installation is done in a transactioned way: If one of the..assemblies fails to install, the installations of all other..assemblies are rolled back. Uninstall is not transactioned.....Options take the form /switch=[value]. Any option that occurs..before the name of an assembly will apply to that assembly's..installation. Options are cumulative but overridable - options..specified for one assembly will apply to the next as well unless..the option is specified with a new value. The default for

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	5.4197749658829855
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:	DINTEC PO.exe
File size:	862720
MD5:	f1d00b68162820d29eb884a91b9e6a09
SHA1:	406621cc2e30d19645513296fe1c5f50dd6c3848
SHA256:	29800b7d8e8c3c60918a37c992a2890b4ccf9e4e0c949accd48821302d0f2891
SHA512:	b9098f02c929f9a59b4adb846b47152d8ee69261d14558t3c2bf3bafd35ac2a81e690c02c1f5dc6f6bef694e4f79f668fbc16a20ab747914c570abe8f22901fe
SSDEEP:	6144:xMpm7XDISoFhkENO4jfCbN898MyDqFNb7LWt+Ao23KB2pTwcSn9vCfEvg4J:xszDNj6u8My+b/WtI23d9ZSn9Vd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L... .,0.....P.....N<.. ...@....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d3c4e
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:	0x302CE720 [Sat Aug 12 17:38:40 1995 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

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
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	0xd3bfc	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x61e	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd6000	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	0xd1c54	0xd1e00	False	0.488976883562	data	5.42525670543	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x61e	0x800	False	0.3515625	data	3.6599210344	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd6000	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	0xd40a0	0x394	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0xd4434	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

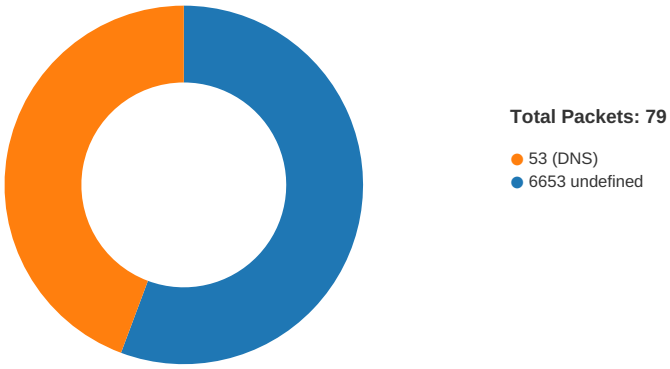
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2017 =?C538IEI@2B=?C?=JB8BDAI
Assembly Version	1.0.0.0
InternalName	PO ALCA.exe
FileVersion	3.5.6.8
CompanyName	=?C538IEI@2B=?C?=JB8BDAI
Comments	BCBIJ6:J@J9:JB:E:D
ProductName	B>;DD:B><B7<9:8JDE8
ProductVersion	3.5.6.8
FileDescription	B>;DD:B><B7<9:8JDE8
OriginalFilename	PO ALCA.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:01:00.952848911 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:01.028206110 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:01.028367043 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:01.114006996 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:01.451936007 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:01.858261108 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:02.561496019 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:03.005784035 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:03.005836010 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:03.089016914 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:03.177653074 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:03.177742004 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:03.561520100 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:03.888801098 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:03.949511051 CET	49741	6653	192.168.2.4	95.181.155.123

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:01:03.962405920 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:04.075752974 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:04.264669895 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:04.769470930 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:04.786421061 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:04.813169956 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:04.813241959 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:04.813321114 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:04.814028978 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:04.842773914 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:04.843736887 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:05.069211960 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.331626892 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.335463047 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.335556030 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:05.337575912 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.341698885 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.344283104 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:05.379535913 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.380742073 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.380809069 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:05.383564949 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.452286005 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:05.577234983 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.764817953 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:05.881474972 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.881515980 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.881599903 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:05.922389984 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.925460100 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.927619934 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:05.929500103 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.931454897 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:05.931540012 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.076910019 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.142680883 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.142771006 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.143799067 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.146528959 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.146584034 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.150599003 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.151644945 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.153623104 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.153649092 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.192765951 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.195647001 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.226119995 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.418000937 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.465146065 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.465230942 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.467014074 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.561733961 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.582814932 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.582904100 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.685321093 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.685368061 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.685444117 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.686191082 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.687038898 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.687164068 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.687232971 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.689173937 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.689677000 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.734419107 CET	6653	49741	95.181.155.123	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:01:06.734477043 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.734509945 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.734543085 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.735380888 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.735491991 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.736346006 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.736386061 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.736419916 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.736452103 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.736489058 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.819372892 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.819490910 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.930474043 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.941236019 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.944252014 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.944380045 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.947284937 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.947316885 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.947406054 CET	49741	6653	192.168.2.4	95.181.155.123
Jan 13, 2021 17:01:06.950398922 CET	6653	49741	95.181.155.123	192.168.2.4
Jan 13, 2021 17:01:06.955533028 CET	6653	49741	95.181.155.123	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:00:25.347143888 CET	49910	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:00:25.403336048 CET	53	49910	8.8.8.8	192.168.2.4
Jan 13, 2021 17:00:26.344784975 CET	55854	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:00:26.392699003 CET	53	55854	8.8.8.8	192.168.2.4
Jan 13, 2021 17:00:27.283121109 CET	64549	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:00:27.331218004 CET	53	64549	8.8.8.8	192.168.2.4
Jan 13, 2021 17:00:28.324155092 CET	63153	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:00:28.372128963 CET	53	63153	8.8.8.8	192.168.2.4
Jan 13, 2021 17:00:29.396509886 CET	52991	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:00:29.452795029 CET	53	52991	8.8.8.8	192.168.2.4
Jan 13, 2021 17:00:54.564604044 CET	53700	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:00:54.612792969 CET	53	53700	8.8.8.8	192.168.2.4
Jan 13, 2021 17:00:58.005304098 CET	51726	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:00:58.053287029 CET	53	51726	8.8.8.8	192.168.2.4
Jan 13, 2021 17:00:58.999053001 CET	56794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:00:59.055248022 CET	53	56794	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:00.013540030 CET	56534	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:00.062360048 CET	53	56534	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:00.868149996 CET	56627	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:00.934649944 CET	53	56627	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:00.951459885 CET	56621	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:01.002295971 CET	53	56621	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:01.622205019 CET	63116	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:01.680059910 CET	53	63116	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:03.095650911 CET	64078	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:03.146430969 CET	53	64078	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:15.299303055 CET	64801	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:15.355711937 CET	53	64801	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:17.906789064 CET	61721	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:17.993438005 CET	53	61721	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:18.579271078 CET	51255	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:18.638320923 CET	53	51255	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:19.392586946 CET	61522	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:19.504714966 CET	53	61522	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:19.661504984 CET	52337	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:19.725918055 CET	53	52337	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:20.164793015 CET	55046	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:20.226536036 CET	53	55046	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:20.765428066 CET	49612	53	192.168.2.4	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 13, 2021 17:01:20.821866035 CET	53	49612	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:21.434371948 CET	49285	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:21.490617037 CET	53	49285	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:22.387001991 CET	50601	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:22.437706947 CET	53	50601	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:24.354434967 CET	60875	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:24.405220985 CET	53	60875	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:24.823137045 CET	56448	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:24.879628897 CET	53	56448	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:25.249605894 CET	59172	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:25.300503969 CET	53	59172	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:25.839740038 CET	62420	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:25.896162033 CET	53	62420	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:26.067039013 CET	60579	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:26.123409986 CET	53	60579	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:26.403696060 CET	50183	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:26.459981918 CET	53	50183	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:27.067111015 CET	61531	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:27.126549006 CET	53	61531	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:27.851475954 CET	49228	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:27.902072906 CET	53	49228	8.8.8.8	192.168.2.4
Jan 13, 2021 17:01:31.775759935 CET	59794	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:01:31.838294983 CET	53	59794	8.8.8.8	192.168.2.4
Jan 13, 2021 17:02:05.329132080 CET	55916	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:02:05.377079964 CET	53	55916	8.8.8.8	192.168.2.4
Jan 13, 2021 17:02:07.006273031 CET	52752	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:02:07.073296070 CET	53	52752	8.8.8.8	192.168.2.4
Jan 13, 2021 17:02:27.355690956 CET	60542	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:02:27.416623116 CET	53	60542	8.8.8.8	192.168.2.4
Jan 13, 2021 17:02:38.157340050 CET	60689	53	192.168.2.4	8.8.8.8
Jan 13, 2021 17:02:38.205274105 CET	53	60689	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 13, 2021 17:01:00.868149996 CET	192.168.2.4	8.8.8.8	0xde7f	Standard query (0)	mnvh54254.ddns.net	A (IP address)	IN (0x0001)
Jan 13, 2021 17:02:27.355690956 CET	192.168.2.4	8.8.8.8	0xc738	Standard query (0)	mnvh54254.ddns.net	A (IP address)	IN (0x0001)

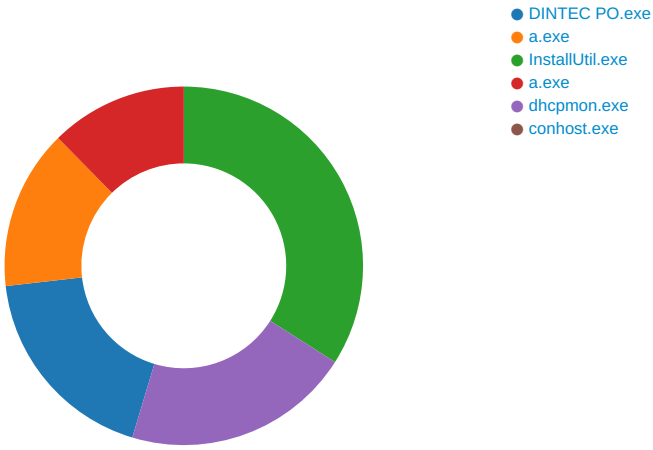
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 13, 2021 17:01:00.934649944 CET	8.8.8.8	192.168.2.4	0xde7f	No error (0)	mnvh54254.ddns.net		95.181.155.123	A (IP address)	IN (0x0001)
Jan 13, 2021 17:02:27.416623116 CET	8.8.8.8	192.168.2.4	0xc738	No error (0)	mnvh54254.ddns.net		95.181.155.123	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: DINTEC PO.exe PID: 4584 Parent PID: 5896

General

Start time:	17:00:30
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\DINTEC PO.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\DINTEC PO.exe'
Imagebase:	0xb40000
File size:	862720 bytes
MD5 hash:	F1D00B68162820D29EB884A91B9E6A09
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: 00000000.00000002.717848221.00000000049AF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.717848221.00000000049AF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.717848221.00000000049AF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.717510555.0000000004819000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.717510555.0000000004819000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.717510555.0000000004819000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	55BC17B	CopyFileExW
C:\Users\user\AppData\Roaming\a.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	55BC17B	CopyFileExW
C:\Users\user\AppData\Roaming\a.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	55BC17B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DINTECPO.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	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	55BC17B	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\a.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 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 20 e7 2c 30 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 1e 0d 00 00 0a 00 00 00 00 00 00 4e 3c 0d 00 00 20 00 00 00 40 0d 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 00 80 0d 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 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode....$.....PE..L... .,0.....P.....N<... ...@....@.. ....`.....	success or wait	4	55BC17B	CopyFileExW
C:\Users\user\AppData\Roaming\a.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	55BC17B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\DINTEC PO.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	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	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	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D0B03DE	ReadFile

Analysis Process: a.exe PID: 6896 Parent PID: 3424

General

Start time:	17:00:46
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Roaming\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\a.exe'
Imagebase:	0x160000
File size:	862720 bytes
MD5 hash:	F1D00B68162820D29EB884A91B9E6A09
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: 00000002.00000002.1055562426.00000000041EF000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.1055562426.00000000041EF000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.1055562426.00000000041EF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.1055335478.0000000004059000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.1055335478.0000000004059000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.1055335478.0000000004059000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.1055038371.0000000003711000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.1055038371.0000000003711000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.1055038371.0000000003711000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6D17CF06	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	6D17CF06	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown

Analysis Process: InstallUtil.exe PID: 6676 Parent PID: 6896

General

Start time:	17:00:53
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0x900000
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, Description: unknown, Source: 00000004.00000003.901015469.0000000004838000.00000004.00000001.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

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	6D17CF06	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	6D17CF06	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	6BFCBEFF	CreateDirectoryW
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	6BFC1E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6BFCBEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	6BFCDD66	CopyFileW
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	6BFCBEFF	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	6BFCBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	2	6BFC1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BFC1E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6BFC1E60	CreateFileW

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	b7 a6 64 6b dc b7 d8 48	..dk...H	success or wait	1	6BFC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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 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 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	6BFCDD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b........4h...t .+..Z\.. .i.......@.3..{...grv +V.....B.......].P...W.4C}uL.. ...s~..F...}.......E......E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	6BFC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_...Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6BFC1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~. .....3.U.	success or wait	1	6BFC1B4F	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D13D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D13D72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	4096	success or wait	1	6D13D72F	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	unknown	512	success or wait	1	6D13D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6BFC646A	RegSetValueExW

Analysis Process: a.exe PID: 6040 Parent PID: 4584

General

Start time:	17:00:54
Start date:	13/01/2021
Path:	C:\Users\user\AppData\Roaming\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\a.exe'
Imagebase:	0x2e0000
File size:	862720 bytes
MD5 hash:	F1D00B68162820D29EB884A91B9E6A09
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\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.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	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll.aux	unknown	2516	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll.aux	unknown	1912	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\WindowsBase\dd5a228cf16a218ff0d3f02cdcbab8c9\WindowsBase.ni.dll.aux	unknown	1348	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xaml\8c85184f1e0cfe359eea86373661a3f8\System.Xaml.ni.dll.aux	unknown	572	success or wait	1	6D0B03DE	ReadFile

Analysis Process: dhcpmon.exe PID: 4904 Parent PID: 3424

General

Start time:	17:01:10
Start date:	13/01/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x8a0000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	6D17CF06	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	6D17CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D48C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	0			success or wait	1	6BFC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	unknown	132	4d 69 63 72 6f 73 6f 66 74 20 28 52 29 20 2e 4e 45 54 20 46 72 61 6d 65 77 6f 72 6b 20 49 6e 73 74 61 6c 6c 61 74 69 6f 6e 20 75 74 69 6c 69 74 79 20 56 65 72 73 69 6f 6e 20 34 2e 37 2e 33 30 35 36 2e 30 0d 0a 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73 65 72 76 65 64 2e 0d 0a 0d 0a	Microsoft (R) .NET Framework Installation utility Version 4. 7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....	success or wait	1	6BFC1B4F	WriteFile
\Device\ConDrv	unknown	256	55 73 61 67 65 3a 20 49 6e 73 74 61 6c 6c 55 74 69 6c 20 5b 2f 75 20 7c 20 2f 75 6e 69 6e 73 74 61 6c 6c 5d 20 5b 6f 70 74 69 6f 6e 20 5b 2e 2e 2e 5d 5d 20 61 73 73 65 6d 62 6c 79 20 5b 5b 6f 70 74 69 6f 6e 20 5b 2e 2e 2e 5d 5d 20 61 73 73 65 6d 62 6c 79 5d 20 5b 2e 2e 2e 5d 5d 0d 0a 0d 0a 49 6e 73 74 61 6c 6c 55 74 69 6c 20 65 78 65 63 75 74 65 73 20 74 68 65 20 69 6e 73 74 61 6c 6c 65 72 73 20 69 6e 20 65 61 63 68 20 67 69 76 65 6e 20 61 73 73 65 6d 62 6c 79 2e 0d 0a 49 66 20 74 68 65 20 2f 75 20 6f 72 20 2f 75 6e 69 6e 73 74 61 6c 6c 20 73 77 69 74 63 68 20 69 73 20 73 70 65 63 69 66 69 65 64 2c 20 69 74 20 75 6e 69 6e 73 74 61 6c 6c 73 0d 0a 74 68 65 20 61 73 73 65 6d 62 6c 69 65 73 2c 20 6f 74 68 65 72 77 69 73 65 20 69 74 20 69 6e 73 74 61 6c 6c 73	Usage: InstallUtil [/u | /uninstall] [option [...]] assembly [[option [...]] assembly] [...]]....InstallUtil executes the installers in each given assembly...If the /u or /uninstall switch is specified, it uninstalls..the assemblies, otherwise it installs	success or wait	7	6BFC1B4F	WriteFile
\Device\ConDrv	unknown	93	69 74 68 20 74 68 65 20 70 61 74 68 73 0d 0a 6f 66 20 74 68 65 20 61 73 73 65 6d 62 6c 69 65 73 20 6f 6e 20 74 68 65 20 63 6f 6d 6d 61 6e 64 20 6c 69 6e 65 20 61 6c 6f 6e 67 20 77 69 74 68 20 74 68 65 20 2f 3f 20 6f 72 20 2f 68 65 6c 70 20 6f 70 74 69 6f 6e 2e 2e 0d 0a 0d 0a 0d 0a	ith the paths..of the assemblies on the command line along with the /? or /help option.....	success or wait	1	6BFC1B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	950	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2e 49 6e 73 74 61 6c 6c 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Configuration.Install, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImage	success or wait	1	6D48C907	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	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: conhost.exe PID: 6128 Parent PID: 4904

General

Start time:	17:01:10
Start date:	13/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis