ID: 382596
Sample Name:
PO_6620200947535257662_Arabico.PDF.exe
Cookbook: default.jbs
Time: 10:35:12
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

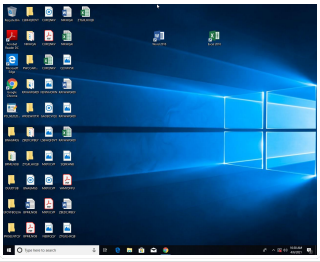
Analysis Report PO_6620200947535257662_Arabico.PD…

Overview

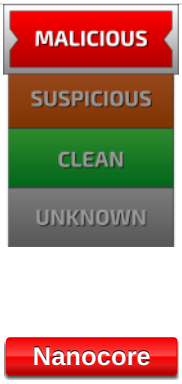
General Information

Sample Name:	PO_6620200947535257662_Arabico.PDF.exe
Analysis ID:	382596
MD5:	b737570f9e9a1bd.
SHA1:	0dd10acab603b2..
SHA256:	0a3a85fd6964b0c.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



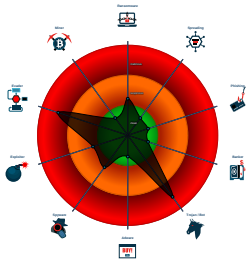
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- Allocates memory in foreign process…
- C2 URLs / IPs found in malware con…
- Creates an undocumented autostart …
- Drops PE files to the user root direc…
- Hides that the sample has been dow…

Classification



Startup

- **System is w10x64**
- PO_6620200947535257662_Arabico.PDF.exe (PID: 6408 cmdline: 'C:\Users\user\Desktop\PO_6620200947535257662_Arabico.PDF.exe' MD5: B737570F9E9A1BDD794F78E3906E61B9)
  - cmd.exe (PID: 6780 cmdline: 'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' /f /v 'Shell' /t REG_SZ /d 'explorer.exe,C:\Users\user\gvvccsccefghhsnd.exe,' MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6788 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - reg.exe (PID: 6816 cmdline: REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' /f /v 'Shell' /t REG_SZ /d 'explorer.exe,C:\Users\user\gvvccsccefghhsnd.exe,' MD5: CEE2A7E57DF2A159A065A34913A055C2)
  - gvvccsccefghhsnd.exe (PID: 6824 cmdline: 'C:\Users\user\gvvccsccefghhsnd.exe' MD5: B737570F9E9A1BDD794F78E3906E61B9)
    - InstallUtil.exe (PID: 5596 cmdline: C:\Users\user\AppData\Local\Temp\InstallUtil.exe MD5: EFEC8C379D165E3F33B536739AEE26A3)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "883c2226-d991-4f34-8646-4dd2732a",
  "Group": "",
  "Domain1": "185.157.161.86",
  "Domain2": "nanopc.linkpc.net",
  "Port": 50005,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001C.00000002.601546888.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001C.00000002.601546888.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001C.00000002.601546888.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000001C.00000002.611212434.000000000597000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000001C.00000002.611212434.000000000597000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
Click to see the 29 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
19.2.gvvccsccefghhsnd.exe.39f9dd8.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

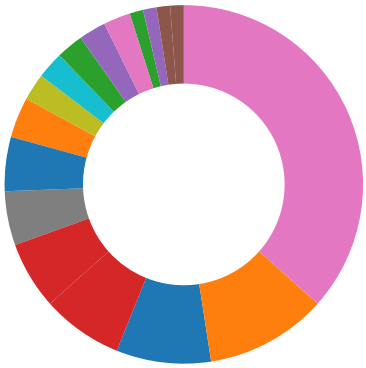
Source	Rule	Description	Author	Strings
19.2.gvvccscccefghhsnd.exe.39f9dd8.7.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
19.2.gvvccscccefghhsnd.exe.39f9dd8.7.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
19.2.gvvccscccefghhsnd.exe.39f9dd8.7.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
0.2.PO_66202009475352576 62_Arabico.PDF.exe.398d830.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 104 entries				

Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview



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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Creates an undocumented autostart registry key

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection:

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

Uses an obfuscated file name to hide its real file extension (double extension)

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:

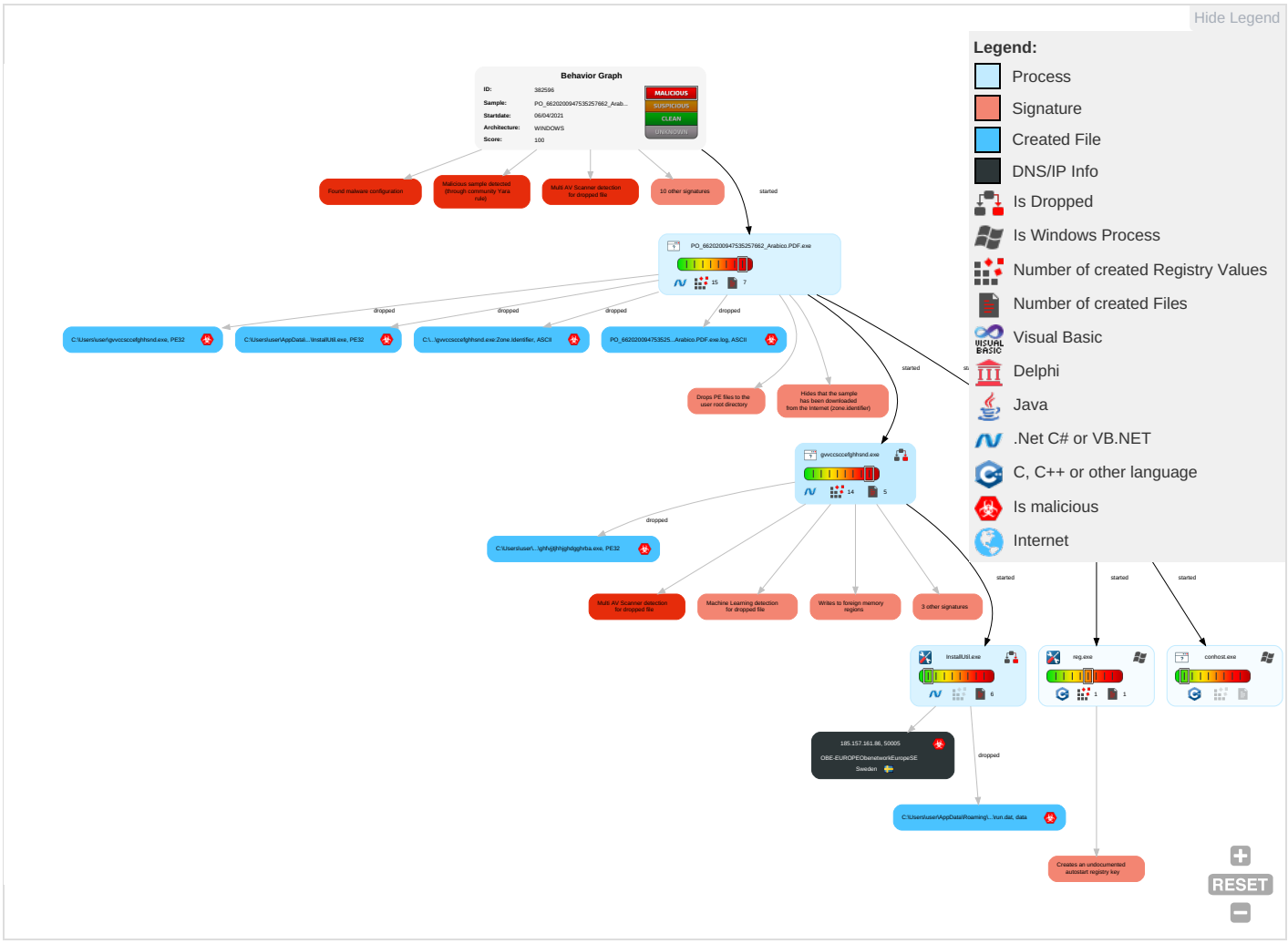
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
Valid Accounts 1	Windows Management Instrumentation	Valid Accounts 1	Valid Accounts 1	Disable or Modify Tools 1	Input Capture 1 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Scheduled Task/Job	Registry Run Keys / Startup Folder 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Nor Por
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 3 1 2	Obfuscated Files or Information 1 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Rer Soft
Local Accounts	At (Windows)	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Software Packing 1 1	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	App Lay Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fall Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 2 1 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
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	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Modify Registry 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Wel
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Virtualization/Sandbox Evasion 3 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Process Injection 3 1 2	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mai
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Hidden Files and Directories 1	Keylogging	Local Groups	Component Object Model and Distributed COM	Screen Capture	Exfiltration over USB	DNS

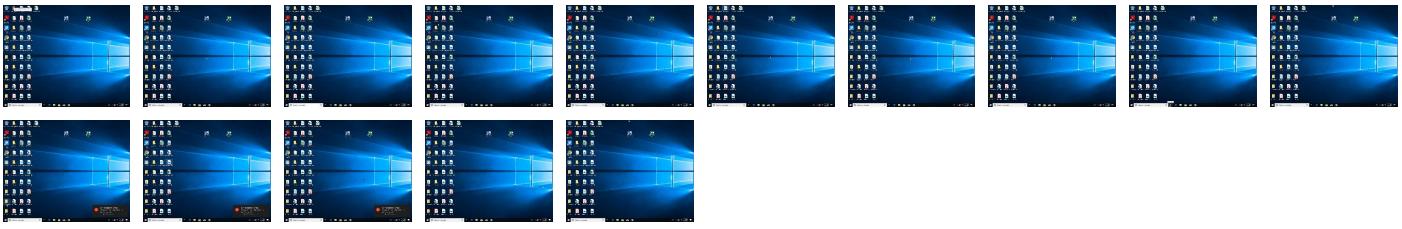
Behavior Graph



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
PO_662020094753525766 2_Arabico.PDF.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PO_662020094753525766 2_Arabico.PDF.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\gvvccsccefghhsnd.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\ghfvjjtjhhjghdgghrba.exe	14%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ghfvjjtjhhjghdgghrba.exe	26%	ReversingLabs	Win32.Trojan.Ymacco	
C:\Users\user\gvvccsccefghhsnd.exe	21%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
28.2.InstallUtil.exe.5970000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
28.2.InstallUtil.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
185.157.161.86	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

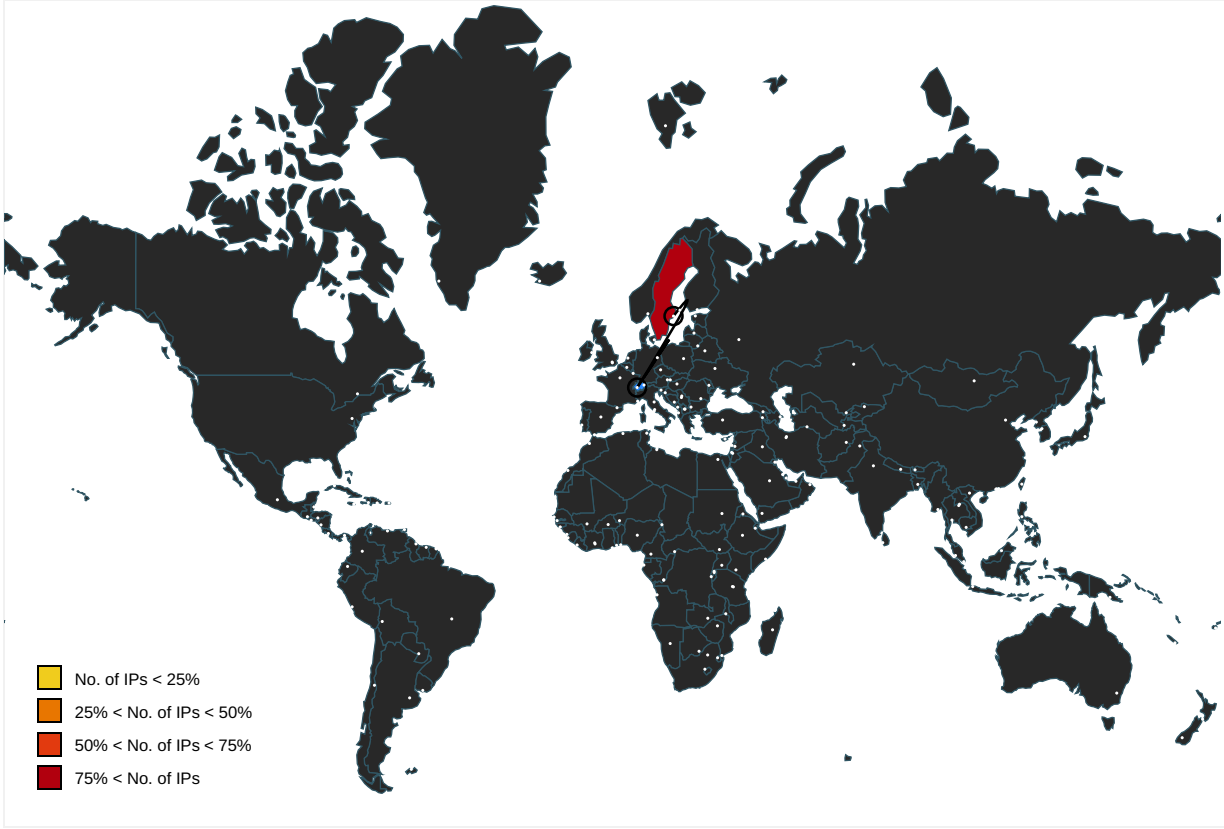
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
nanopc.linkpc.net	false		high
185.157.161.86	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://pki.goog/gsr2/GTS1O1.crt0	PO_6620200947535257662_Arabico .PDF.exe, 00000000.00000002.46 5739066.00000000026EE000.00000 004.00000001.sdmp, gvvccsccefg hhsnd.exe, 00000013.00000002.6 03029028.0000000000A22000.0000 0004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pki.goog/gsr2/gsr2.crl0?	gvvccsccefghhsnd.exe, 00000013 .00000002.603029028.0000000000 A22000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://pki.goog/repository/0	gvvccsccefghhsnd.exe, 00000013 .00000002.603029028.0000000000 A22000.00000004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	PO_6620200947535257662_Arabico .PDF.exe, 00000000.00000002.46 5715365.00000000026C1000.00000 004.00000001.sdmp, gvvccsccefg hhsnd.exe, 00000013.00000002.6 04361409.0000000002731000.0000 0004.00000001.sdmp	false		high
http://schema.org/WebPage	gvvccsccefghhsnd.exe, 00000013 .00000002.604420150.0000000002 75E000.00000004.00000001.sdmp	false		high
http://crl.pki.goog/GTS1O1core.crl0	PO_6620200947535257662_Arabico .PDF.exe, 00000000.00000002.46 5739066.00000000026EE000.00000 004.00000001.sdmp, gvvccsccefg hhsnd.exe, 00000013.00000002.6 03029028.0000000000A22000.0000 0004.00000020.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.157.161.86	unknown	Sweden		197595	OBE-EUROPEObenetworkEuropeSE	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382596
Start date:	06.04.2021
Start time:	10:35:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO_6620200947535257662_Arabico.PDF.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:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/7@0/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0.1%) • Quality average: 22.7% • Quality standard deviation: 26.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 52.255.188.83, 131.253.33.200, 13.107.22.200, 13.64.90.137, 93.184.221.240, 92.122.145.220, 216.58.207.164, 204.79.197.200, 13.107.21.200, 104.43.139.144, 20.82.209.183, 92.122.213.194, 92.122.213.247, 104.42.151.234, 52.155.217.156, 2.20.142.210, 2.20.142.209, 20.54.26.129, 20.50.102.62, 184.30.24.56, 13.88.21.125 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wu.azureedge.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, cs11.wpc.v0cdn.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, www.google.com, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, e1723.g.akamaiedge.net, download.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.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. • VT rate limit hit for: /opt/package/joesandbox/database/analysis/382596/sample/PO_6620200947535257662_Arabico.PDF.exe

Simulations

Behavior and APIs

Time	Type	Description
10:36:25	API Interceptor	227x Sleep call for process: PO_6620200947535257662_Arabico.PDF.exe modified
10:37:23	API Interceptor	188x Sleep call for process: gvvccsccefghhsnd.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.157.161.86	CN-Invoice-XXXXX9808-19011143287998.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287994.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287993.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	
	CN-Invoice-XXXXX9808-19011143287990.exe	Get hash	malicious	Browse	
	Order_List_PO# 081929.exe	Get hash	malicious	Browse	
	order-1812896543124646450.exe	Get hash	malicious	Browse	
	order-181289654312464649.exe	Get hash	malicious	Browse	
	order-181289654312464648.exe	Get hash	malicious	Browse	
	Order_1101201918_AUTECH.exe	Get hash	malicious	Browse	
	50404868-c352-422f-a608-7fd64b335eec.exe	Get hash	malicious	Browse	
	74725794.pdf.exe	Get hash	malicious	Browse	
	Order_List_PO# 0819289.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OBE-EUROPEObenetworkEuropeSE	KUWAIT NATIONAL PETROLEUM COMPANY (KNPC) .pdf.exe	Get hash	malicious	Browse	• 45.148.16.46
	Order PONSB 04042021.pdf(939MB).exe	Get hash	malicious	Browse	• 45.148.16.42
	Document.exe	Get hash	malicious	Browse	• 193.187.90.38
	Swift Copy Against due Invoice.PDF.exe	Get hash	malicious	Browse	• 45.148.16.42
	Ref150420190619A-B0270PEL. pdf.exe	Get hash	malicious	Browse	• 45.148.16.42
	Attached pdf.exe	Get hash	malicious	Browse	• 185.157.160.229
	DHL DELIVERY NOTE 2021003982721.exe	Get hash	malicious	Browse	• 45.148.16.42
	file.exe	Get hash	malicious	Browse	• 217.64.151.217
	0001.exe	Get hash	malicious	Browse	• 185.86.106.202
	0001.exe	Get hash	malicious	Browse	• 185.86.106.202
	PO_6620200947535257653_Arabico.PDF.exe	Get hash	malicious	Browse	• 185.157.161.20
	Purchase Order.exe	Get hash	malicious	Browse	• 185.157.161.113
	FedEx Tracking Details.exe	Get hash	malicious	Browse	• 185.86.106.202
	HBL10909LIT266NR5272RBL2021PRD66178278_LAX2778.PDF.exe	Get hash	malicious	Browse	• 194.32.146.143
	Purchase Order.exe	Get hash	malicious	Browse	• 185.157.161.113
	Nuevo orden & Aliafor Documentos.exe	Get hash	malicious	Browse	• 185.86.106.202
	Document.exe	Get hash	malicious	Browse	• 217.64.151.237
	CN-Invoice-XXXXX9808-19011143287998.exe	Get hash	malicious	Browse	• 185.157.161.20
	Document.exe	Get hash	malicious	Browse	• 217.64.151.237
	Purchase Order.exe	Get hash	malicious	Browse	• 185.157.161.113

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	payment notification.exe	Get hash	malicious	Browse	
	Payment Notification.exe	Get hash	malicious	Browse	
	s.exe	Get hash	malicious	Browse	
	MV.exe	Get hash	malicious	Browse	
	e.exe	Get hash	malicious	Browse	
	SL_PO8192.PDF.exe	Get hash	malicious	Browse	
	QUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	
	RFQ9088QTY.exe	Get hash	malicious	Browse	
	NEWQUOTATION#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe	Get hash	malicious	Browse	
	OUTSTANDING PAYMENT,PDF.exe	Get hash	malicious	Browse	
	New Order 567w43.exe	Get hash	malicious	Browse	
	SRESTKM-series.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.Siggen12.56637.29917.exe	Get hash	malicious	Browse	
	VITR000413774..exe	Get hash	malicious	Browse	
	Order 100955-21042021.exe	Get hash	malicious	Browse	
	R ALHTQ19-P0401-940 GR2P5 TYPBLDG-NASE FERDAN Q0539 NE-Q22.exe	Get hash	malicious	Browse	
	ORDER 100955-21042021.exe	Get hash	malicious	Browse	
	DOCUMENT_395849584954.exe	Get hash	malicious	Browse	
	Documents_00924930493030493.exe	Get hash	malicious	Browse	
	All Details.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_6620200947535257662_Arabico.PDF.exe.log

Process:	C:\Users\user\Desktop\PO_6620200947535257662_Arabico.PDF.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1402
Entropy (8bit):	5.338819835253785
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4bE4Ko84qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKoesX3:MIHK5HKXE1qHbHKovmAHKzvRYHKhQnoe
MD5:	8273F0DD3A6F885D475E92688D9D7583
SHA1:	2DD9D780D4E2F2AD7B458F5A5722D36081F426C4
SHA-256:	D17626929C751206513FE9CF332754F45480CA9E262F746E86D38E6ADD16F8AB
SHA-512:	FB70A91B9B67C2A78D77EBD2B3F8E104664AC97AA4C487CCB90ED3A114A311B46DCD77052CEB184501CECE4A577D952CC479E0AF8F891CB44D2B2C70228C01E
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..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.Co

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

Process:	C:\Users\user\Desktop\PO_6620200947535257662_Arabico.PDF.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

C:\Users\user\AppData\Local\Temp\InstallUtil.exe	
MD5:	EFEC8C379D165E3F33B536739AEE26A3
SHA1:	C875908ACBA5CAC1E0B40F06A83F0F156A2640FA
SHA-256:	46DEE184523A584E56DF93389F81992911A1BA6B1F05AD7D803C6AB1450E18CB
SHA-512:	497847EC115D9AF78899E6DC20EC32A60B16954F83CF5169A23DD3F1459CB632DAC95417BD898FD1895C9FE2262FCBF7838FCF6919FB3B851A0557FBE07CCFF
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: payment notification.exe, Detection: malicious, Browse • Filename: Payment Notification.exe, Detection: malicious, Browse • Filename: s.exe, Detection: malicious, Browse • Filename: MV.exe, Detection: malicious, Browse • Filename: e.exe, Detection: malicious, Browse • Filename: SL_PO8192.PDF.exe, Detection: malicious, Browse • Filename: QUOTATIONs#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe, Detection: malicious, Browse • Filename: RFQ9088QTY.exe, Detection: malicious, Browse • Filename: NEWQUOTATION#280321_RFQ_PRODUCTS_ENQUIRY_TRINITY_VIETNAM_CO.exe, Detection: malicious, Browse • Filename: OUTSTANDING PAYMENT,PDF.exe, Detection: malicious, Browse • Filename: New Order 567w43.exe, Detection: malicious, Browse • Filename: SRESTKM-series.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.Siggen12.56637.29917.exe, Detection: malicious, Browse • Filename: VITR000413774..exe, Detection: malicious, Browse • Filename: Order 100955-21042021.exe, Detection: malicious, Browse • Filename: R ALHTQ19-P0401-940 GR2P5 TYPBLDG-NASE FERDAN Q0539 NE-Q22.exe, Detection: malicious, Browse • Filename: ORDER 100955-21042021.exe, Detection: malicious, Browse • Filename: DOCUMENT_395849584954.exe, Detection: malicious, Browse • Filename: Documents_00924930493030493.exe, Detection: malicious, Browse • Filename: All Details.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\Temp\ghfvjjtjhhjghdgghrba.exe	
Process:	C:\Users\user\gvvccsccefghhsnd.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:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 14%, Browse • Antivirus: ReversingLabs, Detection: 26%
Reputation:	moderate, very likely benign file
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\ghfvjjtjhhjghdgghrba.txt	
Process:	C:\Users\user\gvvccsccefghhsnd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	49
Entropy (8bit):	4.279486946865809
Encrypted:	false
SSDEEP:	3:X8ONEE1Jn:MONEE1Jn
MD5:	C50B8CB81A83FE38A157C2B6099037A3
SHA1:	FC12D6A3FFE15AF1F556278A241A0E6C2C9B99FA
SHA-256:	F7A45394303B3F40F087D96F532DD3D980FAC1B235750420F816DF422B5EB65F
SHA-512:	9519F5FB1EFA2D201690772109ECEBF15DF1F4485D26AE547AE93A115C843D89FEA78B145C55C31405D5E0FFF27131EBBEDBEC490D0DE08740098AA2AC018A13
Malicious:	false

C:\Users\user\AppData\Local\Temp\ghfvjjtjhhjghdgghrba.txt	
Reputation:	low
Preview:	6824..C:\Users\user\gvvccsccefghhsnd.exe..0..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:5Hsn:Zsn
MD5:	F9E71D3F4FE71AEA2CFFFD1007D5C98A
SHA1:	577D0D6A494CDB5DBE47D6ECD4917C05A3448604
SHA-256:	36B9796CEAD21232A868FD8644B236F4BB7775645263371280526609A8AF78AC
SHA-512:	9E3BD49F498FBAD737B0D712BDE57847D6457C29AB84989B9883CA71DD0026E38430C8B4D2F95878EBD8D2B386F86F5BE01DFED029DE1D6BAEEAA6322B1E72 4D
Malicious:	**true**
Reputation:	low
Preview:	d~..''..H

C:\Users\user\gvvccsccefghhsnd.exe	
Process:	C:\Users\user\Desktop\PO_6620200947535257662_Arabico.PDF.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	819712
Entropy (8bit):	6.584112685753224
Encrypted:	false
SSDEEP:	12288:uA1hpIV1Fn6OAVo1TCIV7B+AcieFXe7SIcNo5fqOedXJuL:pG65o12c7BWGSP4fqXK
MD5:	B737570F9E9A1BDD794F78E3906E61B9
SHA1:	0DD10ACAB603B2F1269D05534902B09D38E31AC5
SHA-256:	0A3A85FD6964B0CF1B61E41CC7C117ADA4C8607A0107AD4921DAFA69933EF0AC
SHA-512:	89FF7B15CE9C7D9B689C1C1A72DE630F3EC1DC2B3073818665DE0CB73C879D85ED853F0352BD6DBA93ED14D0674BE95DC726183B1D5218BE2BBA8F488057C4 6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 21%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....M.(..... .....@.. ....`.....@...K..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....p.....H.....<M...m.....,...L.....Y.....E9.....GP*...z....F..l..c.bZ.+$O\.....a.CB...0...)Xq.@.^.r.s.....v.S.y.s)..Y.. bfC.%%.C.....0.C...i.\D.z.G@Jh.L..0gj.....b...CZQ.]. .....nF.....i..+6z1....C.....u6.x9.t....~...|.z./l..._.Q.....1x2.n.>...(..x{{].d7gNaVb..0#...u.$.`..h)W.....J(.....P ...V@.d..>.f.....m..p.....J.ex....}..r.....d.....[.mYZ..[)]k&...Lh.-.uf.. ..o._F....Vc.>jh..g}...+.

C:\Users\user\gvvccsccefghhsnd.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PO_6620200947535257662_Arabico.PDF.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):	6.584112685753224
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:	PO_6620200947535257662_Arabico.PDF.exe
File size:	819712
MD5:	b737570f9e9a1bdd794f78e3906e61b9
SHA1:	0dd10acab603b2f1269d05534902b09d38e31ac5
SHA256:	0a3a85fd6964b0cf1b61e41cc7c117ada4c8607a0107ad4921dafa69933ef0ac
SHA512:	89ff7b15ce9c7d9b689c1c1a72de630f3ec1dc2b3073818665de0cb73c879d85ed853f0352bd6dba93ed14d0674be95dc726183b1d5218be2bba8f488057c446
SSDEEP:	12288:uA1hplV1Fn6OAVo1TClV7B+AcieFXe7SIcNo5fqOedXJuL:pG65o12c7BWGSP4fqXK
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....M.(..... .....@.. ..... .`.....

File Icon

Icon Hash:	c2d2cacad2dac2b5

Static PE Info

General

Entrypoint:	0x4aba8e
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:	0x28EC4D1C [Fri Oct 4 11:14:36 1991 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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xaba40	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xac000	0x1e1ba	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xcc000	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	0xa9a94	0xa9c00	False	0.646130568851	data	6.66011560165	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xac000	0x1e1ba	0x1e200	False	0.31882942168	data	5.62921284867	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xcc000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xac250	0x4b17	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xb0d68	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xc1590	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295		

Name	RVA	Size	Type	Language	Country
RT_ICON	0xc57b8	0x25a8	data		
RT_ICON	0xc7d60	0x10a8	data		
RT_ICON	0xc8e08	0x988	data		
RT_ICON	0xc9790	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xc9bf8	0x68	data		
RT_VERSION	0xc9c60	0x370	data		
RT_MANIFEST	0xc9fd0	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

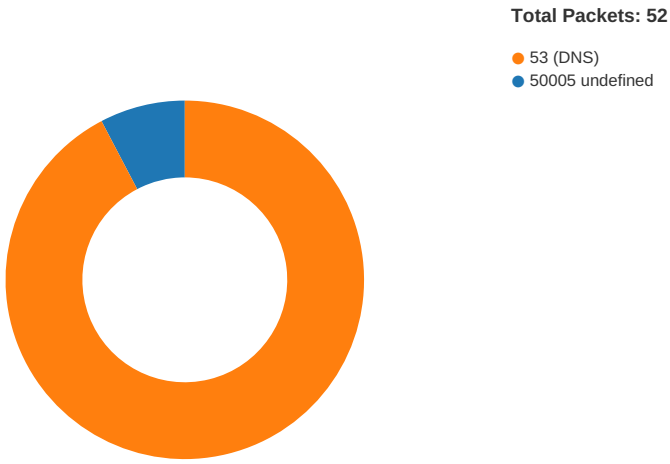
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 1992 AFJJ37@>78:@HDI
Assembly Version	1.0.0.0
InternalName	mcntyre.exe
FileVersion	1.2.2.2
CompanyName	AFJJ37@>78:@HDI
Comments	F57J8JB63IE655B2;:3
ProductName	96B<978J9;I>I72><3
ProductVersion	1.2.2.2
FileDescription	96B<978J9;I>I72><3
OriginalFilename	mcntyre.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/06/21-10:36:02.258188	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/06/21-10:36:02.290439	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
04/06/21-10:36:02.293339	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/06/21-10:36:02.325672	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
04/06/21-10:36:02.326654	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/06/21-10:36:02.364823	ICMP	449	ICMP Time-To-Live Exceeded in Transit			81.95.15.57	192.168.2.6
04/06/21-10:36:02.366540	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/06/21-10:36:02.404984	ICMP	449	ICMP Time-To-Live Exceeded in Transit			152.195.101.202	192.168.2.6
04/06/21-10:36:02.406086	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/06/21-10:36:02.444532	ICMP	449	ICMP Time-To-Live Exceeded in Transit			152.195.101.129	192.168.2.6
04/06/21-10:36:02.445016	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
04/06/21-10:36:02.482920	ICMP	408	ICMP Echo Reply			93.184.221.240	192.168.2.6

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 10:38:01.661478996 CEST	49754	50005	192.168.2.6	185.157.161.86
Apr 6, 2021 10:38:04.667439938 CEST	49754	50005	192.168.2.6	185.157.161.86
Apr 6, 2021 10:38:10.667876959 CEST	49754	50005	192.168.2.6	185.157.161.86
Apr 6, 2021 10:38:20.153971910 CEST	49756	50005	192.168.2.6	185.157.161.86

UDP Packets

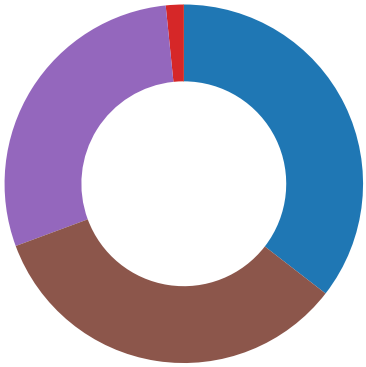
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 10:35:59.397299051 CEST	49283	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:35:59.443243980 CEST	53	49283	8.8.8.8	192.168.2.6
Apr 6, 2021 10:35:59.517369986 CEST	58377	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:35:59.563328028 CEST	53	58377	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:00.804811954 CEST	55074	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:00.853636026 CEST	53	55074	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:02.191914082 CEST	54513	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:02.257329941 CEST	53	54513	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:02.711837053 CEST	62044	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:02.770776987 CEST	53	62044	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:09.553786039 CEST	63791	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:09.602634907 CEST	53	63791	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:09.999507904 CEST	64267	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:10.064980984 CEST	53	64267	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:10.082122087 CEST	49448	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:10.136673927 CEST	53	49448	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:26.339577913 CEST	60342	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:26.396933079 CEST	53	60342	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:27.212419987 CEST	61346	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:27.269778967 CEST	53	61346	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:32.991431952 CEST	51774	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:33.037364006 CEST	53	51774	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:36.954302073 CEST	56023	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:37.012487888 CEST	53	56023	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:45.596035004 CEST	58384	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:45.641974926 CEST	53	58384	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:46.486073017 CEST	60261	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:46.541996956 CEST	53	60261	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:48.242137909 CEST	56061	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:48.290954113 CEST	53	56061	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:49.800721884 CEST	58336	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:49.942778111 CEST	53	58336	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:50.392990112 CEST	53781	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:50.441786051 CEST	53	53781	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:50.506048918 CEST	54064	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:50.569228888 CEST	53	54064	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:51.103629112 CEST	52811	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 10:36:51.158143997 CEST	53	52811	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:51.644021034 CEST	55299	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:51.725781918 CEST	63745	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:51.728620052 CEST	50055	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:51.774887085 CEST	53	50055	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:51.783021927 CEST	53	63745	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:51.787916899 CEST	53	55299	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:51.880153894 CEST	61374	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:51.935127974 CEST	53	61374	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:52.171984911 CEST	50339	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:52.253487110 CEST	53	50339	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:52.340657949 CEST	63307	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:52.386590004 CEST	53	63307	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:52.925522089 CEST	49694	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:52.983159065 CEST	53	49694	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:53.452385902 CEST	54982	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:53.507927895 CEST	53	54982	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:55.018774986 CEST	50010	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:55.067365885 CEST	53	50010	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:56.314537048 CEST	63718	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:56.360495090 CEST	53	63718	8.8.8.8	192.168.2.6
Apr 6, 2021 10:36:56.813999891 CEST	62116	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:36:56.871093988 CEST	53	62116	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:07.923084974 CEST	63816	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:07.968991995 CEST	53	63816	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:08.062706947 CEST	55014	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:08.090409040 CEST	62208	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:08.127232075 CEST	53	55014	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:08.167853117 CEST	53	62208	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:08.515583992 CEST	57574	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:08.561724901 CEST	53	57574	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:08.577095985 CEST	51818	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:08.633795023 CEST	53	51818	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:11.131500006 CEST	56628	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:11.189194918 CEST	53	56628	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:23.345535994 CEST	60778	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:23.391628027 CEST	53	60778	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:33.386636019 CEST	53799	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:33.435512066 CEST	53	53799	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:35.820000887 CEST	54683	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:35.908873081 CEST	53	54683	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:42.182859898 CEST	59329	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:42.228646040 CEST	53	59329	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:43.043751001 CEST	64021	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:43.098184109 CEST	53	64021	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:45.124299049 CEST	56129	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:45.194892883 CEST	53	56129	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:46.069515944 CEST	58177	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:46.115487099 CEST	53	58177	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:53.475512981 CEST	50700	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:53.521442890 CEST	53	50700	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:54.615837097 CEST	54069	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:54.661771059 CEST	53	54069	8.8.8.8	192.168.2.6
Apr 6, 2021 10:37:59.579653025 CEST	61178	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:37:59.626425982 CEST	53	61178	8.8.8.8	192.168.2.6
Apr 6, 2021 10:38:01.148498058 CEST	57017	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:38:01.199031115 CEST	53	57017	8.8.8.8	192.168.2.6
Apr 6, 2021 10:38:05.286000013 CEST	56327	53	192.168.2.6	8.8.8.8
Apr 6, 2021 10:38:05.334856033 CEST	53	56327	8.8.8.8	192.168.2.6

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: PO_6620200947535257662_Arabico.PDF.exe PID: 6408 Parent PID: 5988

General

Start time:	10:36:07
Start date:	06/04/2021
Path:	C:\Users\user\Desktop\PO_6620200947535257662_Arabico.PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PO_6620200947535257662_Arabico.PDF.exe'
Imagebase:	0x240000
File size:	819712 bytes
MD5 hash:	B737570F9E9A1BDD794F78E3906E61B9
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: 00000000.00000002.466854129.00000000037EA000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.466854129.00000000037EA000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.466854129.00000000037EA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.467149528.0000000003947000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.467149528.0000000003947000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.467149528.0000000003947000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ECF06	unknown
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	63F711B	CopyFileExW
C:\Users\user\gvvccsccefghhsnd.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	63F711B	CopyFileExW
C:\Users\user\gvvccsccefghhsnd.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	63F711B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_6620200947535257662_Arabico.PDF.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E3FC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\InstallUtil.exe	0	41064	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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	63F711B	CopyFileExW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\gvvccsccefghhsnd.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 1c 4d ec 28 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 08 00 00 9c 0a 00 00 e4 01 00 00 00 00 00 8e ba 0a 00 00 20 00 00 00 c0 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 e0 0c 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.....M. (................................ ....@.. ....`.................	success or wait	4	63F711B	CopyFileExW
C:\Users\user\gvvccsccefghhsnd.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	63F711B	CopyFileExW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PO_6620200947535257662_Arabico.PDF.exe.log	unknown	1402	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 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 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 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 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E3FC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0C5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0CCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0203DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0203DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0C5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF31B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF31B4F	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6780 Parent PID: 6408

General

Start time:	10:36:22
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	'cmd.exe' /c REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' /f /v 'Shell' /t REG_SZ /d 'explorer.exe,C:\Users\user\gvvccsccefghhsnd.exe,'
Imagebase:	0x2a0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6788 Parent PID: 6780

General

Start time:	10:36:22
Start date:	06/04/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: reg.exe PID: 6816 Parent PID: 6780

General

Start time:	10:36:23
Start date:	06/04/2021
Path:	C:\Windows\SysWOW64\reg.exe
Wow64 process (32bit):	true
Commandline:	REG ADD 'HKCU\Software\Microsoft\Windows NT\CurrentVersion\Winlogon' /f /v 'Shell' /t REG_SZ /d 'explorer.exe,C:\Users\user\gvvccsccefghhsnd.exe,'
Imagebase:	0x10a0000
File size:	59392 bytes
MD5 hash:	CEE2A7E57DF2A159A065A34913A055C2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell	unicode	explorer.exe,C:\Users\user\gvvccsccefghhsnd.exe,	success or wait	1	10A5A1D	RegSetValueExW

Analysis Process: gvvccsccefghhsnd.exe PID: 6824 Parent PID: 6408

General

Start time:	10:37:05
Start date:	06/04/2021
Path:	C:\Users\user\gvvccsccefghhsnd.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\gvvccsccefghhsnd.exe'
Imagebase:	0x340000
File size:	819712 bytes
MD5 hash:	B737570F9E9A1BDD794F78E3906E61B9
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: 00000013.00000002.612087588.00000000039B3000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.612087588.00000000039B3000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.612087588.00000000039B3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.611698378.0000000003738000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.611698378.0000000003738000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.611698378.0000000003738000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000013.00000002.611940927.0000000003856000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.611940927.0000000003856000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.611940927.0000000003856000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 21%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ECF06	unknown
C:\Users\user\AppData\Local\Temp\ghfvjjtjhhjghdgghrba.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6CF31E60	CreateFileW
C:\Users\user\AppData\Local\Temp\ghfvjjtjhhjghdgghrba.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF31E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ghfvjjtjhhjghdgghrba.txt	unknown	49	36 38 32 34 0d 0a 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 67 76 76 63 63 73 63 63 65 66 67 68 68 73 6e 64 2e 65 78 65 0d 0a 30 0d 0a	6824..C:\Users\user\gvvccsccefghhsnd.exe..0..	success or wait	1	6CF31B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\ghfvjjtjhhjghdgghrba.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 10 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	6CF31B4F	WriteFile

File Read

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

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: InstallUtil.exe PID: 5596 Parent PID: 6824

General

Start time:	10:37:55

Start date:	06/04/2021
Path:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\InstallUtil.exe
Imagebase:	0xc80000
File size:	41064 bytes
MD5 hash:	EFEC8C379D165E3F33B536739AEE26A3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000002.601546888.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.601546888.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.601546888.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000002.611212434.0000000005970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000001C.00000002.611212434.0000000005970000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.611212434.0000000005970000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.605270680.0000000004179000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.605270680.0000000004179000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000001C.00000002.610481587.0000000005780000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000001C.00000002.610481587.0000000005780000.00000004.00000001.sdmp, Author: Florian Roth
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ECF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E0ECF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF3BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CF31E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF3BEFF	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF3BEFF	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	64 7e 17 b9 22 f9 d8 48	d~.."..H	success or wait	1	6CF31B4F	WriteFile

File Read

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

Disassembly

Code Analysis