ID: 344664
Sample Name:
PAYMENT_TT_COPYINVOICE001262021.pdf.exe
Cookbook: default.jbs
Time: 21:33:31
Date: 26/01/2021
Version: 31.0.0 Emerald

Table of Contents

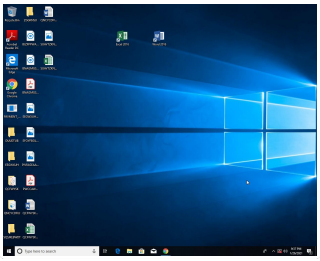
Analysis Report PAYMENT_TT_COPYINVOICE00126202…

Overview

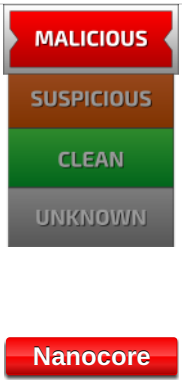
General Information

Sample Name:	PAYMENT_TT_COPYINVOICE001262021.pdf.exe
Analysis ID:	344664
MD5:	84f159a6d9b73e0.
SHA1:	f941d4e4366561b.
SHA256:	69e6c181fa23893.

Most interesting Screenshot:



Detection



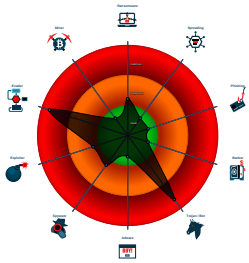
Nanocore

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
- Sigma detected: Scheduled temp file…
- Sigma detected: Suspicious Double …
- Snort IDS alert for network traffic (e…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…

Classification



Startup

- **System is w10x64**
- PAYMENT_TT_COPYINVOICE001262021.pdf.exe (PID: 6008 cmdline: 'C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe' MD5: 84F159A6D9B73E029D2B7E2C34CCCF3B)
  - schtasks.exe (PID: 5720 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KIgtQYTewUpkIc' /XML 'C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PAYMENT_TT_COPYINVOICE001262021.pdf.exe (PID: 4788 cmdline: C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe MD5: 84F159A6D9B73E029D2B7E2C34CCCF3B)
    - schtasks.exe (PID: 5468 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8731.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1124 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PAYMENT_TT_COPYINVOICE001262021.pdf.exe (PID: 2436 cmdline: C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe 0 MD5: 84F159A6D9B73E029D2B7E2C34CCCF3B)
  - schtasks.exe (PID: 5260 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KIgtQYTewUpkIc' /XML 'C:\Users\user\AppData\Local\Temp\tmp4F15.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4784 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PAYMENT_TT_COPYINVOICE001262021.pdf.exe (PID: 5256 cmdline: C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe MD5: 84F159A6D9B73E029D2B7E2C34CCCF3B)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "91.193.75.45"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.624947695.0000000005C90000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000003.00000002.624947695.0000000005C90000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000009.00000002.241857341.000000000455000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000009.00000002.241857341.000000000455000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x4eb0d:$a: NanoCore • 0x4eb66:$a: NanoCore • 0x4eba3:$a: NanoCore • 0x4ec1c:$a: NanoCore • 0x541b1:$a: NanoCore • 0x541fb:$a: NanoCore • 0x543e5:$a: NanoCore • 0x67d04:$a: NanoCore • 0x67d19:$a: NanoCore • 0x67d4e:$a: NanoCore • 0x80ceb:$a: NanoCore • 0x80d00:$a: NanoCore • 0x80d35:$a: NanoCore • 0x4eb6f:$b: ClientPlugin • 0x4ebac:$b: ClientPlugin • 0x4f4aa:$b: ClientPlugin • 0x4f4b7:$b: ClientPlugin • 0x53f4a:$b: ClientPlugin • 0x541ba:$b: ClientPlugin • 0x54204:$b: ClientPlugin • 0x67ac0:$b: ClientPlugin
00000003.00000002.625221873.000000000605000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
Click to see the 36 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.PAYMENT_TT_COPYINVOICE001262021.pdf.exe.5f00000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost
3.2.PAYMENT_TT_COPYINVOICE001262021.pdf.exe.5f00000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1646:$x2: NanoCore.ClientPluginHost • 0x1724:$s4: PipeCreated • 0x1660:$s5: IClientLoggingHost
3.2.PAYMENT_TT_COPYINVOICE001262021.pdf.exe.6050000.7.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
3.2.PAYMENT_TT_COPYINVOICE001262021.pdf.exe.6050000.7.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
3.2.PAYMENT_TT_COPYINVOICE001262021.pdf.exe.6050000.7.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 13 entries				

Sigma Overview

System Summary:

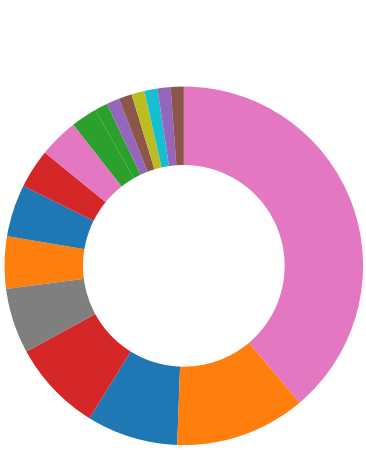
Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Sigma detected: Suspicious Double Extension

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



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

Compliance:

- Uses 32bit PE files
- Uses new MSVCR Dlls
- Contains modern PE file flags such as dynamic base (ASLR) or NX
- Binary contains paths to debug symbols

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)
- Initial sample is a PE file and has a suspicious name

Data Obfuscation:

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

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

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

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

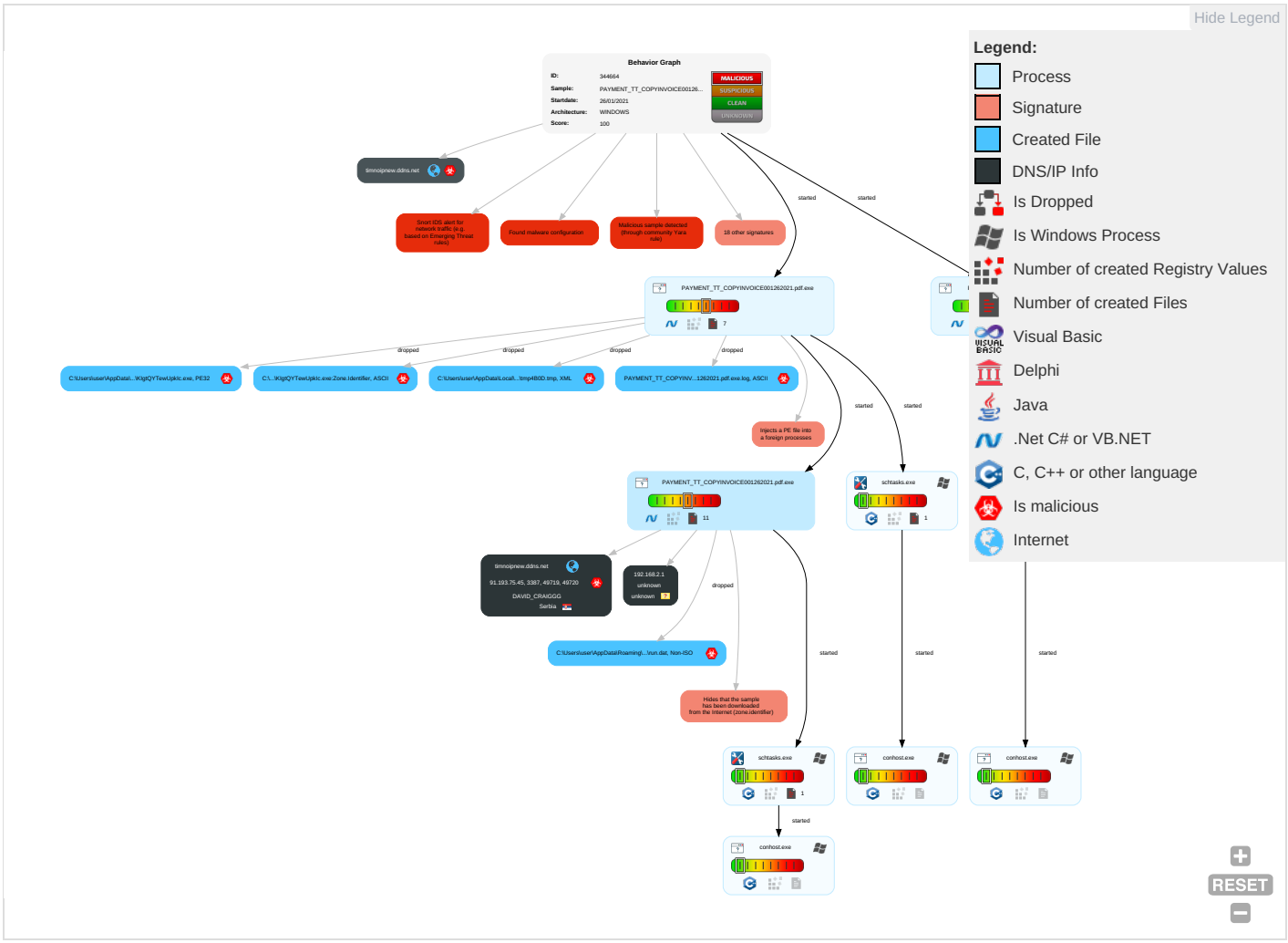
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Valid Accounts	Scheduled Task/Job 1	DLL Side-Loading 1	DLL Side-Loading 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	Ingress Transfer
Default Accounts	Scheduled Task/Job	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 3	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypte Channel
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 1 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Sta Port 1
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Virtualization/Sandbox Evasion 3	SSH	Keylogging	Data Transfer Size Limits	Non-Applicati Layer Protocol
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Applicati Layer Protocol
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commo Used Po
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicati Layer Pr
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	Web Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Trar Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comma and Cor
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	Mail Pro

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
PAYMENT_TT_COPYINVOICE001262021.pdf.exe	42%	Virustotal		Browse
PAYMENT_TT_COPYINVOICE001262021.pdf.exe	9%	ReversingLabs	Win32.Trojan.Pwsx	
PAYMENT_TT_COPYINVOICE001262021.pdf.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.exe	42%	Virustotal		Browse
C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.exe	9%	ReversingLabs	Win32.Trojan.Pwsx	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.PAYMENT_TT_COPYINVOICE001262021.pdf.exe.6050000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
3.2.PAYMENT_TT_COPYINVOICE001262021.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.PAYMENT_TT_COPYINVOICE001262021.pdf.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

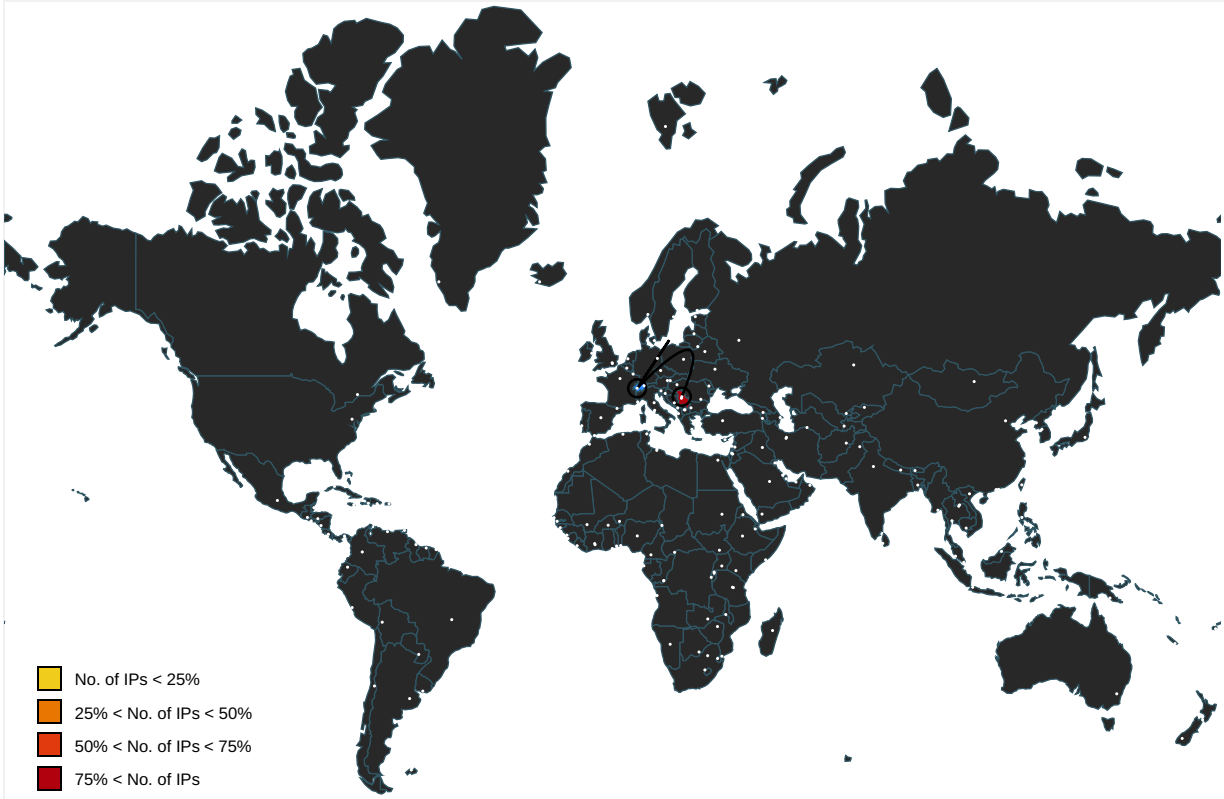
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
timnoipnew.ddns.net	91.193.75.45	true	true		unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
91.193.75.45	unknown	Serbia		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	344664
Start date:	26.01.2021
Start time:	21:33:31
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 14s

Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT_TT_COPYINVOICE001262021.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:	40
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@15/9@32/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
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): MpCmdRun.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • Excluded IPs from analysis (whitelisted): 168.61.161.212, 104.43.193.48, 40.88.32.150, 13.64.90.137, 52.255.188.83, 104.43.139.144, 51.11.168.160, 95.101.22.125, 95.101.22.134, 92.122.253.206, 23.62.99.18, 23.62.99.26, 20.54.26.129, 2.20.157.220, 51.104.139.180, 52.155.217.156 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, displaycatalog.md.mp.microsoft.com.akadns.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:34:22	API Interceptor	1585x Sleep call for process: PAYMENT_TT_COPYINVOICE001262021.pdf.exe modified
21:34:27	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
91.193.75.45	PURCHASE OREDER. PRINT. pdf.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	eTDAg77Nif.exe	Get hash	malicious	Browse	• 91.193.75.94
	hG8XQh9hMy.exe	Get hash	malicious	Browse	• 91.193.75.94
	SecuriteInfo.com.Trojan.Siggen11.59480.29168.exe	Get hash	malicious	Browse	• 91.193.75.94
	qp38gXDG87.exe	Get hash	malicious	Browse	• 91.193.75.94
	Quote#SO2021010197.pdf.exe	Get hash	malicious	Browse	• 91.193.75.185
	SecuriteInfo.com.Trojan.DownLoader36.37095.24479.exe	Get hash	malicious	Browse	• 185.140.53.149
	OTT MT103_211412199807_OP03202101150042_ 20210119_6190008_1.exe	Get hash	malicious	Browse	• 91.193.75.182
	TNT SHIPMENT AWB_IMAGE CI_FROM TNT AWB# 167095453_PDF_____.EXE	Get hash	malicious	Browse	• 91.193.75.155
	9A87wdxsuh.exe	Get hash	malicious	Browse	• 91.193.75.204
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 185.140.53.131
	SecuriteInfo.com.Artemis1A5E2411DEA6.exe	Get hash	malicious	Browse	• 91.193.75.204
	Payment Invoice PDF.exe	Get hash	malicious	Browse	• 185.244.30.18
	New Doc 20211401#_our new price.exe	Get hash	malicious	Browse	• 91.193.75.243
	company profile.exe	Get hash	malicious	Browse	• 185.140.53.227
	NEWORDERrefno0992883jpg.exe	Get hash	malicious	Browse	• 185.140.53.253
	richiealvin.exe	Get hash	malicious	Browse	• 91.193.75.185
	Quotation.exe	Get hash	malicious	Browse	• 185.140.53.154
	DHL Delivery Shipping Cargo. Pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	CompanyLicense.exe	Get hash	malicious	Browse	• 185.140.53.253
	Purchase Order 2094742424.exe	Get hash	malicious	Browse	• 185.244.30.132

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\PAYMENT_TT_COPYINVOICE001262021.pdf.exe.log

Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages _v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp

Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.195355045323717

C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp	
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBatn:cbh47TlNQ//rydbz9l3YODOLNdq36
MD5:	4D74817CFF3E30A5F0AF3D7A0ABCE7B7
SHA1:	CD11190CF9126DCF0FE2B02D5E0DD4592DCC174F
SHA-256:	9B8C81CF1A60FE2F4CFFB754F2A7B28F6CE5E602D55ABE378D17D7B98C0ED3F7
SHA-512:	9C3F42BD404B17B8491FCAAF48294E5B1FFE3C866CA4CEBE00A01A5264702E9E579C61716A032E4B86BD15DF64BB9DC2AFD0F52259725C5FAACAB2C120F4E957
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp4F15.tmp	
Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.195355045323717
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBatn:cbh47TlNQ//rydbz9l3YODOLNdq36
MD5:	4D74817CFF3E30A5F0AF3D7A0ABCE7B7
SHA1:	CD11190CF9126DCF0FE2B02D5E0DD4592DCC174F
SHA-256:	9B8C81CF1A60FE2F4CFFB754F2A7B28F6CE5E602D55ABE378D17D7B98C0ED3F7
SHA-512:	9C3F42BD404B17B8491FCAAF48294E5B1FFE3C866CA4CEBE00A01A5264702E9E579C61716A032E4B86BD15DF64BB9DC2AFD0F52259725C5FAACAB2C120F4E957
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp8731.tmp	
Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1325
Entropy (8bit):	5.168235519124868
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0/+IOk8Vxtn:cbk4oL600QydbQxlYODOLedq383P8Vj
MD5:	9C55D71B6105631C8248121E7083A5DB
SHA1:	F0F576068A4B94B9A110E295FB3C7A0DC00A2294
SHA-256:	02DFB514337664548E807506DA82DBFB23862F20B35640DD2BAF58ECCDFBC0DB
SHA-512:	C82965147A52C8151DC0AEE6F6C8E5196492B80B67B975477247BA5342CEF9352A13EC388209B454E9FBD8AF17438FEE0C058980A561A4E0DE9E1D8BA33102C6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File Type:	data
Category:	dropped
Size (bytes):	1984
Entropy (8bit):	6.997351629001838
Encrypted:	false

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

SSDEEP:	48:IkXCNlkXCNlkXCNlkXCNlkXCNlkXCNlkXCNlkXCg:QRRRRRRk
MD5:	01ACA3E1FB99EBB1C4A590CCF8E5DBF5
SHA1:	B73F827028C10498E94F4442F00D5CA303F0555F
SHA-256:	F131557702B8641631E80AD18CEBFA9B6376A7870629CA4C5386511907BCFF82
SHA-512:	2A02D1A86688C17B39C8EBE2070C6D119D302F0DEC9712391B9D80CA9B0A45E16B59FBA02A149A6FA9BB395E49E6F831BD21754E21531868B2BC314EA34D9A 7
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*............S.Ty.K.&....q$.7....."....F... .N.k.C.X.D.^.....u.\...X........s^.;...m/.,7X.. v"B..#.T.F L...h.....t 5.\|ZGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*............S.Ty.K.&....q$.7....."....F... .N.k.C.X.D.^.....u.\ ...X........s^.;...m/.,7X..v"B..#.T.F L...h.....t 5.|ZGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*............S.Ty.K.&....q$.7....."....F... .N.k.C.X.D.^.....u.\...X........s^.;...m/.,7X..v"B..#.T.F L...h.....t 5.\|ZGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*............S.Ty.K. &....q$.7....."....F... .N.k.C.X.D.^.....u.\...X........s^.;...m/.,7X..v"B..#.T.F L...h.....t 5.|ZGj.h\.3.

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

Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File Type:	Non-ISO extended-ASCII text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:yS1Pn:ycP
MD5:	F29DC7E43E84E1DAC23F0EE480D3B686
SHA1:	1333F272FA4053D8A46980A939DDD4CEF35B98E1
SHA-256:	D4A100D1C2F52263D2ECE5B09A55315E9EE38748A362DF896146696B059AE35E
SHA-512:	D756B64D5D3BA83347A785C7BE30FB11648700DEEDEB05750E94DA28B77D60CFF0D1AB0CE601AF0C734743D73537DBE731FF6477C1BEEDE0FF0779372C89C A3
Malicious:	**true**
Reputation:	low
Preview:	,..5...H

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

Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	62
Entropy (8bit):	4.925576350534983
Encrypted:	false
SSDEEP:	3:oNWXp5v1k+0x6mTKDkFiV2C:oNWXpFu+IOk8kC
MD5:	A9983E872884738EFF30BD9E1876AD24
SHA1:	EA86E75B0D9E93AB4FBD32922E782B8882FA74CB
SHA-256:	C6A3469719B2A1524BD9571E7577E1C15A28D20DD8CF54364C452A5CF289765C
SHA-512:	5187E90A270951A960E256E9AF65CE091C0F0949C0376DDC14178961B56EE95D10BF50BBA63A2E089A9A46001FA5BBAA19C39DD180DC715E34CDA763C7838F1
Malicious:	false
Reputation:	low
Preview:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe

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

Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	560640
Entropy (8bit):	7.678556658487106
Encrypted:	false
SSDEEP:	12288:ZSsJE3bGh84YuU/XM9O+Zss5IKmzmyuvhEyW1WF+pTYS+rTi2tnm071f:ZnE3QjNEslp5CIbWgS+rVZd1
MD5:	84F159A6D9B73E029D2B7E2C34CCCF3B
SHA1:	F941D4E4366561B492273B5D097119F296F7FA22
SHA-256:	69E6C181FA23893493ACDF273050519EEE74C052A8240FB967BFE7BB2D687C2B
SHA-512:	3EADAC075228F4FC4B11B56DE506B8CE0C7116285C2D204FEB986FD6DCFBB2E36B56905510838DBD74DDB600CFAFF595CF1775C1D5D6CB20193870EBEEEA7 B2
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 42%, Browse • Antivirus: ReversingLabs, Detection: 9%
Reputation:	low

C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.W.....P.....n.... ....@.. ..@.....@..B.....P.....H.....K.....(F...[.....0.....(....(.....(.....o!....*.....("....(#.....($.....(%.....(&....*N..(....o....('....*&..((....*.s).....s*.....s+.....s,.....s-.....*....0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0.....~....o2....+..*&..(3....*...0..<.....~.....(4.....,!r...p.....(5...o6...s7.....~.....

C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.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**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.678556658487106
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	PAYMENT_TT_COPYINVOICE001262021.pdf.exe
File size:	560640
MD5:	84f159a6d9b73e029d2b7e2c34cccf3b
SHA1:	f941d4e4366561b492273b5d097119f296f7fa22
SHA256:	69e6c181fa23893493acdf273050519eee74c052a8240fb967bfe7bb2d687c2b
SHA512:	3eadac075228f4fc4b11b56de506b8ce0c7116285c2d204feb986fd6dcfbb2e36b56905510838dbd74ddb600cfaff595cf1775c1d5d6cb20193870ebeeea7ab2
SSDEEP:	12288:ZSsJE3bGh84YuU/XM9O+Zss5IKmzmyuvhEyW1WF+pTYS+rTi2tnm071f:ZnE3QjNEslp5CIbWgS+rVZd1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...'.W.....P.....n.... ....@.. ..@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48a26e
Entrypoint Section:	.text

General

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x9A57B927 [Sun Jan 21 08:58:15 2052 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8a21c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x8c000	0x5ec	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x8a200	0x1c	.text

Name	Virtual Address	Virtual Size	Is in Section
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	0x88274	0x88400	False	0.831024225917	data	7.68934855761	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x8c000	0x5ec	0x600	False	0.431640625	data	4.17333335024	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x8e000	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	0x8c090	0x35c	data		
RT_MANIFEST	0x8c3fc	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 2018
Assembly Version	1.0.0.0
InternalName	LocalDataStoreElement.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	broke-mobile
ProductVersion	1.0.0.0
FileDescription	broke-mobile
OriginalFilename	LocalDataStoreElement.exe

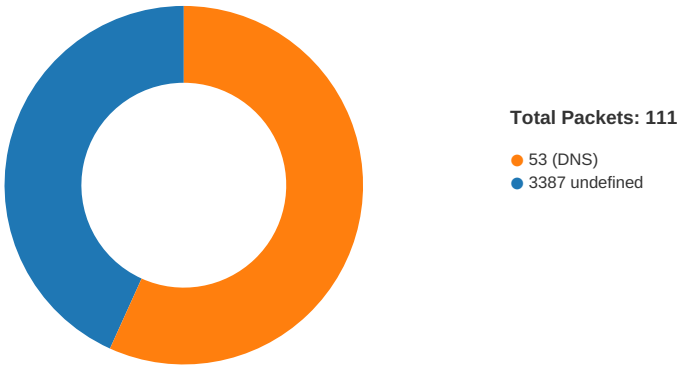
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-21:34:28.539168	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	3387	192.168.2.3	91.193.75.45
01/26/21-21:34:34.822502	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	3387	192.168.2.3	91.193.75.45
01/26/21-21:34:41.361541	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	3387	192.168.2.3	91.193.75.45
01/26/21-21:34:47.620554	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	3387	192.168.2.3	91.193.75.45
01/26/21-21:34:53.794741	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	3387	192.168.2.3	91.193.75.45

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/21-21:35:00.021001	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:06.184662	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:12.464819	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:18.625120	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:24.918080	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:31.191644	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:37.527166	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:43.789996	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:51.101138	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	3387	192.168.2.3	91.193.75.45
01/26/21-21:35:57.314843	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:03.569450	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:09.731186	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:15.904502	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:22.070901	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:28.538558	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:34.753076	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:42.895678	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:49.314662	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	3387	192.168.2.3	91.193.75.45
01/26/21-21:36:55.583749	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	3387	192.168.2.3	91.193.75.45
01/26/21-21:37:02.078984	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	3387	192.168.2.3	91.193.75.45
01/26/21-21:37:08.619524	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	3387	192.168.2.3	91.193.75.45
01/26/21-21:37:15.154244	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	3387	192.168.2.3	91.193.75.45
01/26/21-21:37:21.330291	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	3387	192.168.2.3	91.193.75.45
01/26/21-21:37:27.620885	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	3387	192.168.2.3	91.193.75.45
01/26/21-21:37:33.801755	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	3387	192.168.2.3	91.193.75.45

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:34:28.221275091 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:28.508975029 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:28.509073019 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:28.539167881 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:28.840147972 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:28.843693018 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:29.171382904 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:29.171475887 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:29.458030939 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:29.458127975 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:29.794974089 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:29.795252085 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.123100042 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.123217106 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.164719105 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.164767027 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.164804935 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.164870024 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.164917946 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.164925098 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.165018082 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.165055990 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.165092945 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.165101051 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.165128946 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.165148973 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.165179014 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.165185928 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.165256977 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.165294886 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.165333986 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.165345907 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.165359020 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.165410042 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.386796951 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.453315020 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.453368902 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.453421116 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.453457117 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454128981 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454174042 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454204082 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454211950 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454277039 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454279900 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454318047 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454349041 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454368114 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454410076 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454430103 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454447031 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454483986 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454511881 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454524040 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454561949 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454561949 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454602957 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454632044 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454639912 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454691887 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454711914 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454736948 CET	3387	49719	91.193.75.45	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:34:30.454762936 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454775095 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454843998 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:30.454891920 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.454927921 CET	3387	49719	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:30.455013990 CET	49719	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:34.519819021 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:34.815891027 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:34.816118956 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:34.822501898 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:35.125354052 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:35.125446081 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:35.472032070 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:35.476351976 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:35.770724058 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:35.775935888 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.126689911 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.127995968 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.469949007 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.470155001 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.502815008 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.502872944 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.502912998 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.502949953 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.502983093 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.502986908 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.503005981 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.503022909 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.503025055 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.503073931 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.503076077 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.503083944 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.503115892 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.503154039 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.503175974 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.503185987 CET	49720	3387	192.168.2.3	91.193.75.45
Jan 26, 2021 21:34:36.503190041 CET	3387	49720	91.193.75.45	192.168.2.3
Jan 26, 2021 21:34:36.503209114 CET	49720	3387	192.168.2.3	91.193.75.45

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:34:16.855967045 CET	60100	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:16.872390985 CET	53	60100	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:17.654673100 CET	53195	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:17.669891119 CET	53	53195	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:18.489129066 CET	50141	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:18.504183054 CET	53	50141	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:19.314449072 CET	53023	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:19.332118988 CET	53	53023	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:20.715987921 CET	49563	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:20.734266996 CET	53	49563	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:21.511385918 CET	51352	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:21.526686907 CET	53	51352	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:22.318942070 CET	59349	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:22.334333897 CET	53	59349	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:23.135422945 CET	57084	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:23.150850058 CET	53	57084	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:24.478683949 CET	58823	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:24.493927956 CET	53	58823	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:25.302822113 CET	57568	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:25.318388939 CET	53	57568	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:28.194581032 CET	50540	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:28.211956024 CET	53	50540	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:34:34.498286009 CET	54366	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:34.518697977 CET	53	54366	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:41.047509909 CET	53034	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:41.067560911 CET	53	53034	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:41.857954025 CET	57762	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:41.873091936 CET	53	57762	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:44.503434896 CET	55435	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:44.520620108 CET	53	55435	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:47.308022022 CET	50713	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:47.325588942 CET	53	50713	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:50.223699093 CET	56132	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:50.266227007 CET	53	56132	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:53.483220100 CET	58987	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:53.502099991 CET	53	58987	8.8.8.8	192.168.2.3
Jan 26, 2021 21:34:59.687489033 CET	56579	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:34:59.705272913 CET	53	56579	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:05.578206062 CET	60633	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:05.595531940 CET	53	60633	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:05.868284941 CET	61292	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:05.885848999 CET	53	61292	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:12.155966997 CET	63619	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:12.171849012 CET	53	63619	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:16.564371109 CET	64938	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:16.579802036 CET	53	64938	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:18.313263893 CET	61946	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:18.331748009 CET	53	61946	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:19.363354921 CET	64910	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:19.384030104 CET	53	64910	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:24.607584000 CET	52123	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:24.625030994 CET	53	52123	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:30.867216110 CET	56130	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:30.885668039 CET	53	56130	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:37.206720114 CET	56338	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:37.223685026 CET	53	56338	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:43.469353914 CET	59420	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:43.488487005 CET	53	59420	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:49.687550068 CET	58784	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:50.690193892 CET	58784	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:50.706217051 CET	53	58784	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:51.467000008 CET	63978	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:51.485899925 CET	53	63978	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:56.995178938 CET	62938	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:57.015609980 CET	53	62938	8.8.8.8	192.168.2.3
Jan 26, 2021 21:35:59.864432096 CET	55708	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:35:59.888310909 CET	53	55708	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:01.496521950 CET	56803	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:01.515527964 CET	53	56803	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:03.261023998 CET	57145	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:03.277000904 CET	53	57145	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:09.420207024 CET	55359	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:09.436007023 CET	53	55359	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:15.591367960 CET	58306	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:15.611401081 CET	53	58306	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:21.753237963 CET	64124	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:21.771533012 CET	53	64124	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:28.224842072 CET	49361	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:28.242247105 CET	53	49361	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:34.440299988 CET	63150	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:34.456792116 CET	53	63150	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:40.845942020 CET	53279	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:41.865894079 CET	53279	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:42.592725039 CET	53	53279	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:43.745194912 CET	56881	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:43.760828972 CET	53	56881	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2021 21:36:44.074570894 CET	53642	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:44.101372004 CET	53	53642	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:48.966114044 CET	55667	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:48.983299017 CET	53	55667	8.8.8.8	192.168.2.3
Jan 26, 2021 21:36:55.268508911 CET	54833	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:36:55.286046982 CET	53	54833	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:01.744647980 CET	62476	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:01.760329962 CET	53	62476	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:03.007324934 CET	49705	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:03.024019957 CET	53	49705	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:03.376055002 CET	61477	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:03.406825066 CET	53	61477	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:03.812606096 CET	61633	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:03.830101967 CET	53	61633	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:04.539793015 CET	55949	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:04.555706978 CET	53	55949	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:06.214651108 CET	57601	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:06.231595039 CET	53	57601	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:06.691870928 CET	49342	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:06.707829952 CET	53	49342	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:07.018578053 CET	56253	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:07.034485102 CET	53	56253	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:07.423369884 CET	49667	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:07.440964937 CET	53	49667	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:07.880471945 CET	55439	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:07.896198988 CET	53	55439	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:08.139673948 CET	57069	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:08.157744884 CET	53	57069	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:08.308775902 CET	57659	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:08.326914072 CET	53	57659	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:14.834070921 CET	54717	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:14.853471994 CET	53	54717	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:21.018053055 CET	63975	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:21.036380053 CET	53	63975	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:27.226201057 CET	56639	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:27.242166996 CET	53	56639	8.8.8.8	192.168.2.3
Jan 26, 2021 21:37:33.492626905 CET	51856	53	192.168.2.3	8.8.8.8
Jan 26, 2021 21:37:33.508668900 CET	53	51856	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 21:34:28.194581032 CET	192.168.2.3	8.8.8.8	0x1a99	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:34.498286009 CET	192.168.2.3	8.8.8.8	0x8f16	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:41.047509909 CET	192.168.2.3	8.8.8.8	0x726e	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:47.308022022 CET	192.168.2.3	8.8.8.8	0xac82	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:53.483220100 CET	192.168.2.3	8.8.8.8	0x40f8	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:59.687489033 CET	192.168.2.3	8.8.8.8	0x1750	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:05.868284941 CET	192.168.2.3	8.8.8.8	0xaf2d	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:12.155966997 CET	192.168.2.3	8.8.8.8	0xcaad	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:18.313263893 CET	192.168.2.3	8.8.8.8	0x1c64	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:24.607584000 CET	192.168.2.3	8.8.8.8	0xcdc8	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:30.867216110 CET	192.168.2.3	8.8.8.8	0xc3cf	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:37.206720114 CET	192.168.2.3	8.8.8.8	0x735b	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:43.469353914 CET	192.168.2.3	8.8.8.8	0x89b5	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2021 21:35:49.687550068 CET	192.168.2.3	8.8.8.8	0xefe2	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:50.690193892 CET	192.168.2.3	8.8.8.8	0xefe2	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:56.995178938 CET	192.168.2.3	8.8.8.8	0xb81c	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:03.261023998 CET	192.168.2.3	8.8.8.8	0xbdc1	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:09.420207024 CET	192.168.2.3	8.8.8.8	0x8a77	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:15.591367960 CET	192.168.2.3	8.8.8.8	0x2a28	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:21.753237963 CET	192.168.2.3	8.8.8.8	0xca81	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:28.224842072 CET	192.168.2.3	8.8.8.8	0x8c6e	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:34.440299988 CET	192.168.2.3	8.8.8.8	0x1bfa	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:40.845942020 CET	192.168.2.3	8.8.8.8	0xc888	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:41.865894079 CET	192.168.2.3	8.8.8.8	0xc888	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:48.966114044 CET	192.168.2.3	8.8.8.8	0x4d33	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:55.268508911 CET	192.168.2.3	8.8.8.8	0xf9cc	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:01.744647980 CET	192.168.2.3	8.8.8.8	0x8cbf	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:08.308775902 CET	192.168.2.3	8.8.8.8	0xbbbc	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:14.834070921 CET	192.168.2.3	8.8.8.8	0x3e62	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:21.018053055 CET	192.168.2.3	8.8.8.8	0xb719	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:27.226201057 CET	192.168.2.3	8.8.8.8	0xae80	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:33.492626905 CET	192.168.2.3	8.8.8.8	0x2904	Standard query (0)	timnoipnew .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

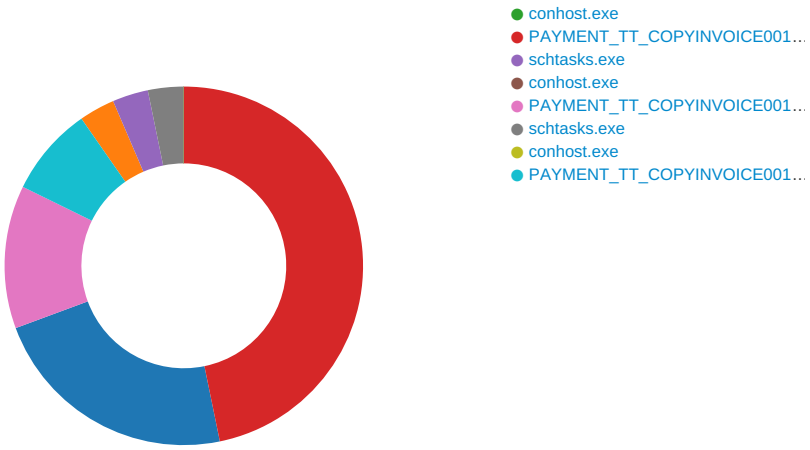
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 21:34:28.211956024 CET	8.8.8.8	192.168.2.3	0x1a99	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:34.518697977 CET	8.8.8.8	192.168.2.3	0x8f16	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:41.067560911 CET	8.8.8.8	192.168.2.3	0x726e	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:47.325588942 CET	8.8.8.8	192.168.2.3	0xac82	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:53.502099991 CET	8.8.8.8	192.168.2.3	0x40f8	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:34:59.705272913 CET	8.8.8.8	192.168.2.3	0x1750	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:05.885848999 CET	8.8.8.8	192.168.2.3	0xaf2d	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:12.171849012 CET	8.8.8.8	192.168.2.3	0xcaad	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:18.331748009 CET	8.8.8.8	192.168.2.3	0x1c64	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:24.625030994 CET	8.8.8.8	192.168.2.3	0xcdc8	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:30.885668039 CET	8.8.8.8	192.168.2.3	0xc3cf	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2021 21:35:37.223685026 CET	8.8.8.8	192.168.2.3	0x735b	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:43.488487005 CET	8.8.8.8	192.168.2.3	0x89b5	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:50.706217051 CET	8.8.8.8	192.168.2.3	0xefe2	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:35:57.015609980 CET	8.8.8.8	192.168.2.3	0xb81c	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:03.277000904 CET	8.8.8.8	192.168.2.3	0xbdc1	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:09.436007023 CET	8.8.8.8	192.168.2.3	0x8a77	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:15.611401081 CET	8.8.8.8	192.168.2.3	0x2a28	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:21.771533012 CET	8.8.8.8	192.168.2.3	0xca81	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:28.242247105 CET	8.8.8.8	192.168.2.3	0x8c6e	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:34.456792116 CET	8.8.8.8	192.168.2.3	0x1bfa	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:42.592725039 CET	8.8.8.8	192.168.2.3	0xc888	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:48.983299017 CET	8.8.8.8	192.168.2.3	0x4d33	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:36:55.286046982 CET	8.8.8.8	192.168.2.3	0xf9cc	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:01.760329962 CET	8.8.8.8	192.168.2.3	0x8cbf	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:08.326914072 CET	8.8.8.8	192.168.2.3	0xbbbc	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:14.853471994 CET	8.8.8.8	192.168.2.3	0x3e62	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:21.036380053 CET	8.8.8.8	192.168.2.3	0xb719	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:27.242166996 CET	8.8.8.8	192.168.2.3	0xae80	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)
Jan 26, 2021 21:37:33.508668900 CET	8.8.8.8	192.168.2.3	0x2904	No error (0)	timnoipnew .ddns.net		91.193.75.45	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: PAYMENT_TT_COPYINVOICE001262021.pdf.exe PID: 6008 Parent PID: 5724

General

Start time:	21:34:22
Start date:	26/01/2021
Path:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe'
Imagebase:	0xa50000
File size:	560640 bytes
MD5 hash:	84F159A6D9B73E029D2B7E2C34CCCF3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.217488646.00000000031E8000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.217645175.0000000004171000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.217645175.0000000004171000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.217645175.0000000004171000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.217424729.0000000003171000.00000004.00000001.sdmp, Author: Joe Security
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	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	72FB60AC	unknown
C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.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	726193EB	unknown
C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	726193EB	unknown
C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	54907D8	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\PAYMENT_TT_COPYINVOICE001262021.pdf.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp	success or wait	1	5490DAA	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 27 b9 57 9a 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 84 08 00 00 08 00 00 00 00 00 00 6e a2 08 00 00 20 00 00 00 c0 08 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 09 00 00 02 00 00 00 00 00 00 02 00 40 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...'.W........... ....P.............n.... ....@.. ....@................	success or wait	3	726193EB	unknown
C:\Users\user\AppData\Roaming\KIgtQYTewUpkIc.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	726193EB	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp	unknown	1647	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	5490A67	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\PAYMENT_TT_COPYINVOICE001262021.pdf.exe.log	unknown	664	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 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 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 23 5c 63 64 37 63 37 34 66 63 65 32 61 30 65 61 62 37 32 63 64 32 35 63 62 65 34 62 62 36 31 36 31 34 5c 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2e 6e	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.n	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: schtasks.exe PID: 5720 Parent PID: 6008

General

Start time:	21:34:23
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KIgtQYTewUpkIc' /XML 'C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp'
Imagebase:	0xe40000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp	unknown	2	success or wait	1	E4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4B0D.tmp	unknown	1648	success or wait	1	E4ABD9	ReadFile

Analysis Process: conhost.exe PID: 5988 Parent PID: 5720

General

Start time:	21:34:24
Start date:	26/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PAYMENT_TT_COPYINVOICE001262021.pdf.exe PID: 4788 Parent PID: 6008

General

Start time:	21:34:25
Start date:	26/01/2021
Path:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
Imagebase:	0xd00000
File size:	560640 bytes
MD5 hash:	84F159A6D9B73E029D2B7E2C34CCCF3B

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: 00000003.00000002.624947695.0000000005C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.624947695.0000000005C90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.625221873.0000000006050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.625221873.0000000006050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.625221873.0000000006050000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.623216945.000000000459F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.616162634.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.616162634.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.616162634.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.625122849.0000000005F00000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.625122849.0000000005F00000.00000004.00000001.sdmp, Author: Florian Roth
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	72FB60AC	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	72FB60AC	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	31807A1	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	318089B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp8731.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	3180B6C	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	318089B	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	31807A1	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	31807A1	CreateDirectoryW
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	72FB60AC	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	72FB60AC	unknown
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	28	318089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8731.tmp	success or wait	1	72637D95	unknown
C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe:Zone.Identifier	success or wait	1	3180F9D	DeleteFileA

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	2c 99 f7 35 85 c2 d8 48	,..5...H	success or wait	1	3180A53	WriteFile
C:\Users\user\AppData\Local\Temp\tmp8731.tmp	unknown	1325	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>	success or wait	1	3180A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	unknown	62	43 3a 5c 55 73 65 72 73 5c 68 61 72 64 7a 5c 44 65 73 6b 74 6f 70 5c 50 41 59 4d 45 4e 54 5f 54 54 5f 43 4f 50 59 49 4e 56 4f 49 43 45 30 30 31 32 36 32 30 32 31 2e 70 64 66 2e 65 78 65	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe	success or wait	1	3180A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	248	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 bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 b0 f9 9a 0b bd fc a3 d0 89 94 e6 53 d6 54 79 e5 83 4b bd 26 f1 d3 e4 a5 0f 71 24 9d 37 8d c1 a6 ba 0b 22 a1 1d 8d d0 9e 46 9f bd 17 20 0e 4e f1 a8 6b f1 b9 43 97 58 c6 44 f7 5e 10 ed 12 fe f6 75 cd 5c 8e ed a5 d3 92 58 10 b2 7f 1d d3 8d b3 7f e2 73 5e ee 3b 9a 2e bf 6d 2f e7 2c 37 58 01 ca 83 76 22 42 ea 7f 23 e5 54 1d 46 20 4c ef 97 83 9f ba 68 f7 9f c2 8f a7 87 74 20 35 1d 7c 5a	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ....S.Ty..K.&.....q$.7. ....".....F... .N..k..C.X.D.^. ....u.\.....X.....s^.;...m /.,7X...v"B..#.T.F L.....h.... ..t 5.|Z	success or wait	8	3180A53	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	3180A53	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7308BF06	unknown

Analysis Process: schtasks.exe PID: 5468 Parent PID: 4788

General

Start time:	21:34:26
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp8731.tmp'
Imagebase:	0xe40000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp8731.tmp	unknown	2	success or wait	1	E4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp8731.tmp	unknown	1326	success or wait	1	E4ABD9	ReadFile

Analysis Process: conhost.exe PID: 1124 Parent PID: 5468

General

Start time:	21:34:26
Start date:	26/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PAYMENT_TT_COPYINVOICE001262021.pdf.exe PID: 2436 Parent PID: 528

General

Start time:	21:34:27
Start date:	26/01/2021
Path:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe 0
Imagebase:	0x40000
File size:	560640 bytes
MD5 hash:	84F159A6D9B73E029D2B7E2C34CCCF3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.227636059.000000000275E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.227909192.0000000003721000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.227909192.0000000003721000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.227909192.0000000003721000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000006.00000002.227611167.0000000002721000.00000004.00000001.sdmp, Author: Joe Security
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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Temp\tmp4F15.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	4A40310	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4F15.tmp	success or wait	1	4A408E2	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4F15.tmp	unknown	1647	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">..<RegistrationInfo>..<Date>2014-10-25T14:27:44.8929027</Date>..<Author>computer\user</Author>..</RegistrationIn	success or wait	1	4A4059F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: schtasks.exe PID: 5260 Parent PID: 2436

General

Start time:	21:34:29
Start date:	26/01/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KIgtQYTewUpkIc' /XML 'C:\Users\user\AppData\Local\Temp\tmp4F15.tmp'
Imagebase:	0xe40000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4F15.tmp	unknown	2	success or wait	1	E4AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp4F15.tmp	unknown	1648	success or wait	1	E4ABD9	ReadFile

Analysis Process: conhost.exe PID: 4784 Parent PID: 5260

General

Start time:	21:34:29
Start date:	26/01/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PAYMENT_TT_COPYINVOICE001262021.pdf.exe PID: 5256 Parent PID: 2436

General

Start time:	21:34:30
Start date:	26/01/2021
Path:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PAYMENT_TT_COPYINVOICE001262021.pdf.exe
Imagebase:	0xde0000
File size:	560640 bytes
MD5 hash:	84F159A6D9B73E029D2B7E2C34CCCF3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.241857341.0000000004551000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.241857341.0000000004551000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.240020828.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.240020828.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.240020828.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.241805191.0000000003551000.00000004.00000001.sdmp, Author: Joe Security
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	72FB60AC	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	72FB60AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Disassembly

Code Analysis