ID: 433326
Sample Name: PAYMENT-PO#987654567.exe
Cookbook: default.jbs
Time: 16:33:18
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

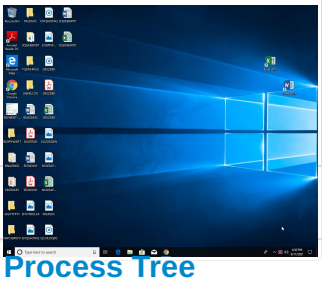
Analysis Report PAYMENT-PO#987654567.exe

Overview

General Information

Sample Name:	PAYMENT-PO#987654567.exe
Analysis ID:	433326
MD5:	568727e4104e3f3.
SHA1:	d693795cbc34b9..
SHA256:	b1cd32f68858de3.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

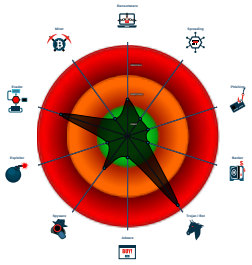
Nanocore

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 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…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …

Classification



Process Tree

- **System is w10x64**
- PAYMENT-PO#987654567.exe (PID: 5372 cmdline: 'C:\Users\user\Desktop\PAYMENT-PO#987654567.exe' MD5: 568727E4104E3F3E56A1368AF64E9248)
  - RegAsm.exe (PID: 3568 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - schtasks.exe (PID: 1400 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpAB2D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5588 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpB06D.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 2968 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegAsm.exe (PID: 3136 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe 0 MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 5456 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 4492 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 4652 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5844 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
  - conhost.exe (PID: 2840 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "fa01d1ff-8193-42b2-a0e1-b0e6c90b",
  "Group": "PO-#9874567",
  "Domain1": "doc-file.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 7755,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.492063110.00000000063E0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000003.00000002.492063110.00000000063E0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000003.00000002.486565092.0000000002EB1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000003.00000000.223604786.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000003.00000000.223604786.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 24 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.RegAsm.exe.3f00624.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
3.2.RegAsm.exe.3f00624.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
3.2.RegAsm.exe.3f00624.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.2.RegAsm.exe.6470000.9.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
3.2.RegAsm.exe.6470000.9.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
Click to see the 60 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicious Process Start Without DLL

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

.NET source code contains very large strings

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

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)

HIPS / PFW / Operating System Protection Evasion:

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

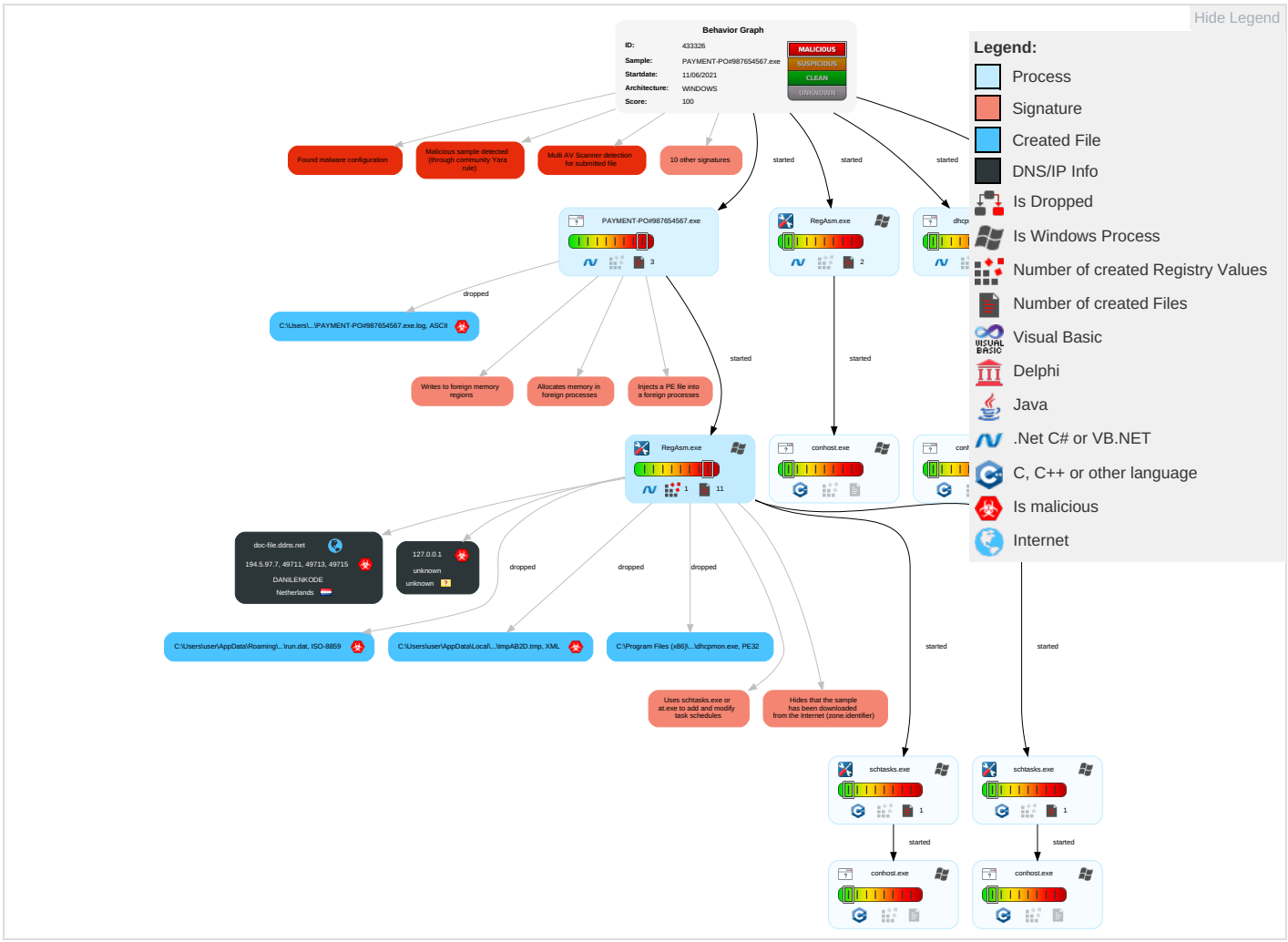
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Command and Scripting Interpreter 2	Scheduled Task/Job 1	Process Injection 3 1 2	Masquerading 2	Input Capture 1 1	Security Software Discovery 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eave Insec Netw Com
Default Accounts	Scheduled Task/Job 1	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explo Track Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 3 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Proto

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	DLL Side-Loading 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

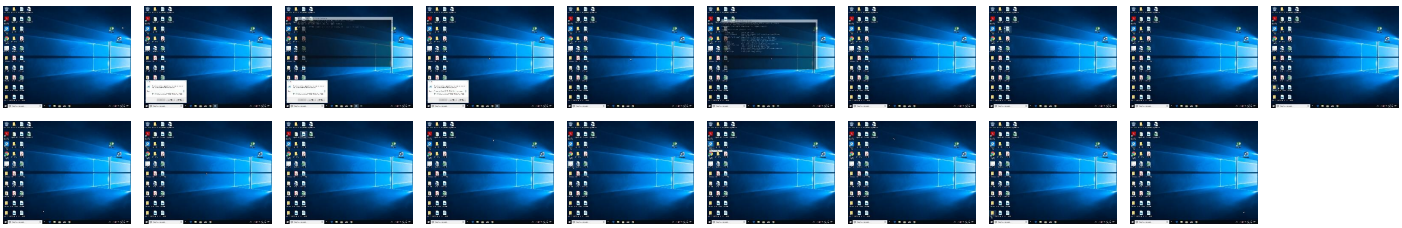
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PAYMENT-PO#987654567.exe	41%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
PAYMENT-PO#987654567.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.RegAsm.exe.6470000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
3.0.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.RegAsm.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
doc-file.ddns.net	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
doc-file.ddns.net	194.5.97.7	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
doc-file.ddns.net	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.7	doc-file.ddns.net	Netherlands		208476	DANILENKODE	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433326
Start date:	11.06.2021
Start time:	16:33:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT-PO#987654567.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:	33
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@15/11@13/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.9% (good quality ratio 0.7%) • Quality average: 58.9% • Quality standard deviation: 30.7%
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

Simulations

Behavior and APIs

Time	Type	Description
16:34:10	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe" s>$(Arg0)
16:34:10	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:34:11	API Interceptor	1017x Sleep call for process: RegAsm.exe modified
16:34:13	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.7	8RJwUlmBjb.exe	Get hash	malicious	Browse	
	B882ITuiXnqLLeM.exe	Get hash	malicious	Browse	
	Doc_43795379326436.PDF.exe	Get hash	malicious	Browse	
	aqa4dSbdFYw5DlK.exe	Get hash	malicious	Browse	
	IITuGuCnGifznoN.exe	Get hash	malicious	Browse	
	IITuGuCnGifznoN.exe	Get hash	malicious	Browse	
	RAHIM TRADING CO. FOR IMP.exe	Get hash	malicious	Browse	
	RAHIM TRADING CO. FOR IMP. & EXP.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	OUTSTANDING INVOICE.pdf.exe	Get hash	malicious	Browse	• 194.5.98.28
	Request Letter for Courtesy Call.xlsx	Get hash	malicious	Browse	• 194.5.97.61
	SecuriteInfo.com.Heur.23766.xls	Get hash	malicious	Browse	• 194.5.97.241
	SwiftCopy.pdf.exe	Get hash	malicious	Browse	• 194.5.98.31
	wlCqbMRJ7p.exe	Get hash	malicious	Browse	• 194.5.98.5
	SecuriteInfo.com.Trojan.PackedNET.832.3222.exe	Get hash	malicious	Browse	• 194.5.98.144
	SecuriteInfo.com.Trojan.PackedNET.831.12541.exe	Get hash	malicious	Browse	• 194.5.98.144
	0Cg1YYs1sv.exe	Get hash	malicious	Browse	• 194.5.98.144
	Duplicated Orders.xlsx	Get hash	malicious	Browse	• 194.5.98.144
	DEPOSITAR.xlsx	Get hash	malicious	Browse	• 194.5.98.144
	InvoicePOzGlybgcIc1vHasG.exe	Get hash	malicious	Browse	• 194.5.98.87
	POInvoiceOrderIuVvcl0VWEOAmXy.exe	Get hash	malicious	Browse	• 194.5.98.87
	payment invoice.exe	Get hash	malicious	Browse	• 194.5.98.23
	#RFQ ORDER484475577797.exe	Get hash	malicious	Browse	• 194.5.98.120

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	b6yzWugw8V.exe	Get hash	malicious	Browse	• 194.5.98.107
	0041#Receipt.pif.exe	Get hash	malicious	Browse	• 194.5.98.180
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.18
	SecuriteInfo.com.Trojan.PackedNET.820.24493.exe	Get hash	malicious	Browse	• 194.5.97.61

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	n3sQ7uTU8v.exe	Get hash	malicious	Browse	
	20014464370.PDF.exe	Get hash	malicious	Browse	
	aXgdOUvL9L.exe	Get hash	malicious	Browse	
	DHL#DOCUMENTS001010.PDF.exe	Get hash	malicious	Browse	
	kyIfnzzg3E.exe	Get hash	malicious	Browse	
	flyZab7hHk.exe	Get hash	malicious	Browse	
	AedJpyQ9lM.exe	Get hash	malicious	Browse	
	UPDATED SOA.exe	Get hash	malicious	Browse	
	qdFDmi3Bhy.exe	Get hash	malicious	Browse	
	RFQ27559404D4E5A.PDF.exe	Get hash	malicious	Browse	
	Receiptn.exe	Get hash	malicious	Browse	
	PURCHASE LIST.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Trojan.PackedNET.783.10804.exe	Get hash	malicious	Browse	
	Y6k2VgaGck.exe	Get hash	malicious	Browse	
	Bank swift.exe	Get hash	malicious	Browse	
	tT1XWdxOYv.exe	Get hash	malicious	Browse	
	363IN050790620 BOOKING.exe	Get hash	malicious	Browse	
	New Order.exe	Get hash	malicious	Browse	
	RFQ#21040590409448.pdf.exe	Get hash	malicious	Browse	
	DHL#DOCUMENTS02010910.PDF.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	64616
Entropy (8bit):	6.037264560032456
Encrypted:	false
SSDEEP:	768:J8XcJiMjm2ieHlPyCsSuJbn8dBhFVBSMQ6Iq8TSYDKpgLaDViRLNdr:9YMaNylPYSAb8dBnTHv8DKKaDVkX
MD5:	6FD7592411112729BF6B1F2F6C34899F
SHA1:	5E5C839726D6A43C478AB0B95DBF52136679F5EA
SHA-256:	FFE4480CCC81B061F725C54587E9D1BA96547D27FE28083305D75796F2EB3E74
SHA-512:	21EFCC9DEE3960F1A64C6D8A44871742558666BB792D77ACE91236C7DBF42A6CA77086918F363C4391D9C00904C55A952E2C18BE5FA1A67A509827BFC630070
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: n3sQ7uTU8v.exe, Detection: malicious, Browse • Filename: 20014464370.PDF.exe, Detection: malicious, Browse • Filename: aXgdOUvL9L.exe, Detection: malicious, Browse • Filename: DHL#DOCUMENTS001010.PDF.exe, Detection: malicious, Browse • Filename: kyIfnzzg3E.exe, Detection: malicious, Browse • Filename: flyZab7hHk.exe, Detection: malicious, Browse • Filename: AedJpyQ9lM.exe, Detection: malicious, Browse • Filename: UPDATED SOA.exe, Detection: malicious, Browse • Filename: qdFDmi3Bhy.exe, Detection: malicious, Browse • Filename: RFQ27559404D4E5A.PDF.exe, Detection: malicious, Browse • Filename: Receiptn.exe, Detection: malicious, Browse • Filename: PURCHASE LIST.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Trojan.PackedNET.783.10804.exe, Detection: malicious, Browse • Filename: Y6k2VgaGck.exe, Detection: malicious, Browse • Filename: Bank swift.exe, Detection: malicious, Browse • Filename: tT1XWdxOYv.exe, Detection: malicious, Browse • Filename: 363IN050790620 BOOKING.exe, Detection: malicious, Browse • Filename: New Order.exe, Detection: malicious, Browse • Filename: RFQ#21040590409448.pdf.exe, Detection: malicious, Browse • Filename: DHL#DOCUMENTS02010910.PDF.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...xX.Z.....0.....^.... .....@.. ....`.....O.....8.....h>..... ..... ..H.....text...d.... ..... ..`.rsrc...8.....@..@.reloc..... .....@..B.....@.....H.....A...p.....T.....~P...-.r...p.....(....(....s.....P...*..0..".....(.....-.r...p.rl..p(....s....z.*...0.....(....~P....o..... .*..(....*n(.....(.....%...(....*~(.....(.....%...%...(....*.(.....(.....%...%...%...(....*V.(.....}Q.....}R...*..{Q...*..{R...*...0.....(.....i.=...}S.....i.@...}T.....i.@...}U.....+m...(....o .....r]..p.o!...,..{T.....{U.....o"....+(.ra..p.o!....,..{T.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\PAYMENT-PO#987654567.exe.log	
Process:	C:\Users\user\Desktop\PAYMENT-PO#987654567.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	706
Entropy (8bit):	5.342604339328228
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPk21rkvoDLI4MWuCq1KDLI4Mq92n4M9XKbbDLI4MWuPJKiUrRZT:ML9E4Ks29E4Kx1qE4x84qXKDE4KhK3Vt
MD5:	9C1DF7CA80077C63698DCFE531754F1F
SHA1:	44E2DE975BF1364781A2E5EDE576D1FBCD948097
SHA-256:	78D4E6F15372E7DFE7C9D5C10BB515995A20AFAEF839C56E750CC336620BCFAB
SHA-512:	7078AFFB531F2AA5C813FB259C113CB1A02C992F76C47AAE036B8591C65EB4A2037B3BDAD83BBD4D30FA7D2CE244D9943C18EA8AA668FEBCD52B864E7476F84D
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",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..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegAsm.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177CE
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	42
Entropy (8bit):	4.0050635535766075
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUy:Q3La/xwQ

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
MD5:	84CFDB4B995B1DBF543B26B86C863ADC
SHA1:	D2F47764908BF30036CF8248B9FF5541E2711FA2
SHA-256:	D8988D672D6915B46946B28C06AD8066C50041F6152A91D37FFA5CF129CC146B
SHA-512:	485F0ED45E13F00A93762CBF15B4B8F996553BAA021152FAE5ABA051E3736BCD3CA8F4328F0E6D9E3E1F910C96C4A9AE055331123EE08E3C2CE3A99AC2E177C E
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..

C:\Users\user\AppData\Local\Temp\tmpAB2D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.134254141338449
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mxz5xtn:cbk4oL600QydbQxIYODOLedq3Zxz5j
MD5:	48EF7FA9033389AD7929D7A6B9D10298
SHA1:	9DB6CB7325C8BDF66A15F7B5F34703709A45AEB6
SHA-256:	0C1B5F67EEB276D1D4205B138CE32BC6149924E02281A2DB8E4623A700E88F15
SHA-512:	AC8BD104ECBACC9BCCCE9E087F67E5B18072D59367CCD31D4E66132B6BAAEA520CBA5B9B59464483D86ABF74826B382C402F12E9A586C99BDA8C78A0DE339 44E
Malicious:	**true**
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\Local\Temp\tmpB06D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
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\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:v8:k
MD5:	A09FCDB23ECE19528BB7449345BC185D
SHA1:	DF1A8BD907EAE6723B67752B8330CE89361CE405
SHA-256:	8045AC16130B0AF030BFD8B43098B481F800223AB711D58F8C51BF4C25CA2020
SHA-512:	3355DCCD1642C89520507000E95D81B46B8C0A2041506F0564EC15F5D900E1AACC2DA66B1B456EE22E7EEE129C337D14B1ACD47FFE86B0C1CFDD167DBB1FA CA
Malicious:	**true**

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Preview:	...h1-.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.823079645651109
Encrypted:	false
SSDEEP:	3:oMty8WddSWAnPL4A:oMLW6WAnPL4A
MD5:	743A1D76D284D8E42E19061A3F13A723
SHA1:	D6BBE641CBAC7B46C0922F32DCC89F8F5B87F98C
SHA-256:	86093BF03032ACFCEF934A0D8363B66AAF4ADEE58015DA0172E13635B1DD1FE8
SHA-512:	DF687DCD985D1F6127624220083DFD93A39FEBCE02A869F4126787DF3724890ECC10FF18077BFDEF02FCC802440F3F83545E4DA4BD826DC84E59B26A105F656
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1049
Entropy (8bit):	4.2989523990568035
Encrypted:	false
SSDEEP:	24:z3U3g4DO/0XZd3Wo3opQ5ZKBQFYVgt7ovrNOYlK:zEw4DBXZxo4ABV+SrUYE
MD5:	970EE6AEAB63008333D1D883327DA660
SHA1:	A71E19F66886B1888A183BA1777A23FABAE9822E
SHA-256:	D270D397EB3CF1173D25795834B240466EFEE213E11B1B31CDC101015AFFCAD9
SHA-512:	EB49AEE1B4524E6F15C08345A380D7D28DC845DEBA5408A7D034F2F7F5A652C8A2E2FF293BFB307DE87DCC2FAA111BA3BE8BEF9C4752A73DE1835DCD844D3BB
Malicious:	false
Preview:	Microsoft .NET Framework Assembly Registration Utility version 4.7.3056.0..for Microsoft .NET Framework version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....Syntax: RegAsm AssemblyName [Options]..Options:.. /unregister Unregister types.. /tlb[:FileName] Export the assembly to the specified type library.. and register it.. /regfile[:FileName] Generate a reg file with the specified name.. instead of registering the types. This option.. cannot be used with the /u or /tlb options.. /codebase Set the code base in the registry.. /registered Only refer to already registered type libraries.. /asmpath:Directory Look for assembly references here.. /nologo Prevents RegAsm from displaying logo.. /silent Silent mode. Prevents displaying of success messages.. /verbose Displays extra information..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	4.798704714965638
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:	PAYMENT-PO#987654567.exe
File size:	1438208
MD5:	568727e4104e3f3e56a1368af64e9248
SHA1:	d693795cbc34b9e49b1ace9581771e24e2d09f3c
SHA256:	b1cd32f68858de3be8e43093dcc24b32b2ce00890857362a652f3e74cebb791c
SHA512:	999340520a456aa62317fb7ea87b3902d6eabbeb739aeb8a7b30b99f60155fa25794390d3691d0dcdabe964df0d8d1282dc51d0bc4dbe9f6ae75ebe489ab66f
SSDEEP:	12288:GY7M3pV+bJAx980BoMM48zYWSqd98i/76FjtNAJwDLHaRPPMC2FQFjBqRxmygNcz:TgtehTZZEMSXA6aUcfsp8QgmD40X

General

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....0.....B.....n.... .....@.. .....@.....@.....

File Icon

Icon Hash:	81c0c1a14931c4c8

Static PE Info

General

Entrypoint:	0x52cd6e
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
Time Stamp:	0x60B71CB7 [Wed Jun 2 05:52:55 2021 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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x12ad74	0x12ae00	False	0.47861528257	data	4.07686014064	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x12e000	0x33e34	0x34000	False	0.437903771034	data	5.71331335745	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x162000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 16:34:11.893193960 CEST	192.168.2.5	8.8.8.8	0x331a	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:17.823801994 CEST	192.168.2.5	8.8.8.8	0xdaa0	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:23.310085058 CEST	192.168.2.5	8.8.8.8	0x2584	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:24.311016083 CEST	192.168.2.5	8.8.8.8	0x2584	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:45.071463108 CEST	192.168.2.5	8.8.8.8	0x9a51	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:50.553538084 CEST	192.168.2.5	8.8.8.8	0xcdf7	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:56.180087090 CEST	192.168.2.5	8.8.8.8	0x3456	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:16.610714912 CEST	192.168.2.5	8.8.8.8	0x5163	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:21.906044006 CEST	192.168.2.5	8.8.8.8	0x380c	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:27.181557894 CEST	192.168.2.5	8.8.8.8	0x2a55	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:48.314888000 CEST	192.168.2.5	8.8.8.8	0x7a90	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:53.658956051 CEST	192.168.2.5	8.8.8.8	0x13c2	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:59.050698042 CEST	192.168.2.5	8.8.8.8	0xd6cb	Standard query (0)	doc-file.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 16:34:11.955162048 CEST	8.8.8.8	192.168.2.5	0x331a	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:17.885736942 CEST	8.8.8.8	192.168.2.5	0xdaa0	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:24.372126102 CEST	8.8.8.8	192.168.2.5	0x2584	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:45.130167961 CEST	8.8.8.8	192.168.2.5	0x9a51	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:50.615031958 CEST	8.8.8.8	192.168.2.5	0xcdf7	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:34:56.238449097 CEST	8.8.8.8	192.168.2.5	0x3456	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:16.670631886 CEST	8.8.8.8	192.168.2.5	0x5163	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:21.969640017 CEST	8.8.8.8	192.168.2.5	0x380c	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:27.241269112 CEST	8.8.8.8	192.168.2.5	0x2a55	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:48.374574900 CEST	8.8.8.8	192.168.2.5	0x7a90	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:53.722754002 CEST	8.8.8.8	192.168.2.5	0x13c2	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)
Jun 11, 2021 16:35:59.114793062 CEST	8.8.8.8	192.168.2.5	0xd6cb	No error (0)	doc-file.ddns.net		194.5.97.7	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PAYMENT-PO#987654567.exe PID: 5372 Parent PID: 5700

General

Start time:	16:34:05
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\PAYMENT-PO#987654567.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\PAYMENT-PO#987654567.exe'
Imagebase:	0x880000
File size:	1438208 bytes
MD5 hash:	568727E4104E3F3E56A1368AF64E9248
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: 00000000.00000002.225391808.000000000406B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.225391808.000000000406B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.225391808.000000000406B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.225536432.0000000004169000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.225536432.0000000004169000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.225536432.0000000004169000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: RegAsm.exe PID: 3568 Parent PID: 5372

General

Start time:	16:34:06
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Imagebase:	0xb40000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
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: 00000003.00000002.492063110.00000000063E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.492063110.00000000063E0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.486565092.0000000002EB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.223604786.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.223604786.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.223604786.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.484697410.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.484697410.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.484697410.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.492128185.0000000006470000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.492128185.0000000006470000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.492128185.0000000006470000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.223324621.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.223324621.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.223324621.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.489761514.0000000003EF9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.489761514.0000000003EF9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 1400 Parent PID: 3568

General

Start time:	16:34:08
Start date:	11/06/2021
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\tmpAB2D.tmp'
Imagebase:	0xd90000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4960 Parent PID: 1400

General

Start time:	16:34:09
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: schtasks.exe PID: 5588 Parent PID: 3568

General

Start time:	16:34:10
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmpB06D.tmp'
Imagebase:	0xd90000
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

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 2968 Parent PID: 5588

General

Start time:	16:34:10
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: RegAsm.exe PID: 3136 Parent PID: 904

General

Start time:	16:34:10
Start date:	11/06/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe 0
Imagebase:	0x7ff797770000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5456 Parent PID: 3136

General

Start time:	16:34:11
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: dhcpmon.exe PID: 4492 Parent PID: 904

General

Start time:	16:34:13
Start date:	11/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xc10000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 4652 Parent PID: 4492

General

Start time:	16:34:13
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: dhcpmon.exe PID: 5844 Parent PID: 3472

General

Start time:	16:34:18
Start date:	11/06/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true

Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x2d0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 2840 Parent PID: 5844

General

Start time:	16:34:19
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis