ID: 452441
Sample Name: Document.1-xml.eml.exe
Cookbook: default.jbs
Time: 11:09:09
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

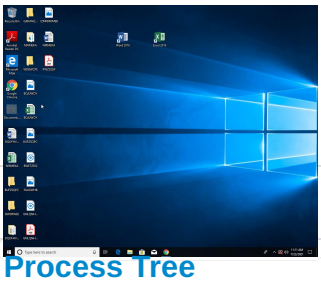
Windows Analysis Report Document.1-xml.eml.exe

Overview

General Information

Sample Name:	Document.1-xml.eml.exe
Analysis ID:	452441
MD5:	4d48e3cbfc19b57..
SHA1:	4863e913b2e570..
SHA256:	45cf5d850ca6806..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

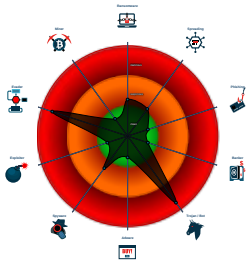
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- Document.1-xml.eml.exe (PID: 6608 cmdline: 'C:\Users\user\Desktop\Document.1-xml.eml.exe' MD5: 4D48E3CBFC19B5729B6C7A968A957805)
  - Document.1-xml.eml.exe (PID: 5768 cmdline: 'C:\Users\user\Desktop\Document.1-xml.eml.exe' MD5: 4D48E3CBFC19B5729B6C7A968A957805)
    - schtasks.exe (PID: 5796 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp3A3F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5960 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5720 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp3DCA.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5288 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Document.1-xml.eml.exe (PID: 5540 cmdline: C:\Users\user\Desktop\Document.1-xml.eml.exe 0 MD5: 4D48E3CBFC19B5729B6C7A968A957805)
- dhcpmon.exe (PID: 5556 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 4D48E3CBFC19B5729B6C7A968A957805)
- dhcpmon.exe (PID: 5608 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 4D48E3CBFC19B5729B6C7A968A957805)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ec07ca6b-08b1-47be-b65b-f4ac1e81",
  "Group": "alozzzz",
  "Domain1": "194.5.98.136",
  "Domain2": "",
  "Port": 2888,
  "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
0000000F.00000002.925419136.00000000052F0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
0000000F.00000002.925419136.00000000052F0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
0000000F.00000002.925419136.00000000052F0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000F.00000001.798397653.000000000402000.00000040.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000001.798397653.000000000402000.00000040.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.Document.1-xml.eml.exe.5050000.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
15.2.Document.1-xml.eml.exe.5050000.6.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
0.2.Document.1-xml.eml.exe.5915a0.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
0.2.Document.1-xml.eml.exe.5915a0.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
0.2.Document.1-xml.eml.exe.5915a0.1.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 41 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

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

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Executable has a suspicious name (potential lure to open the executable)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

.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)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

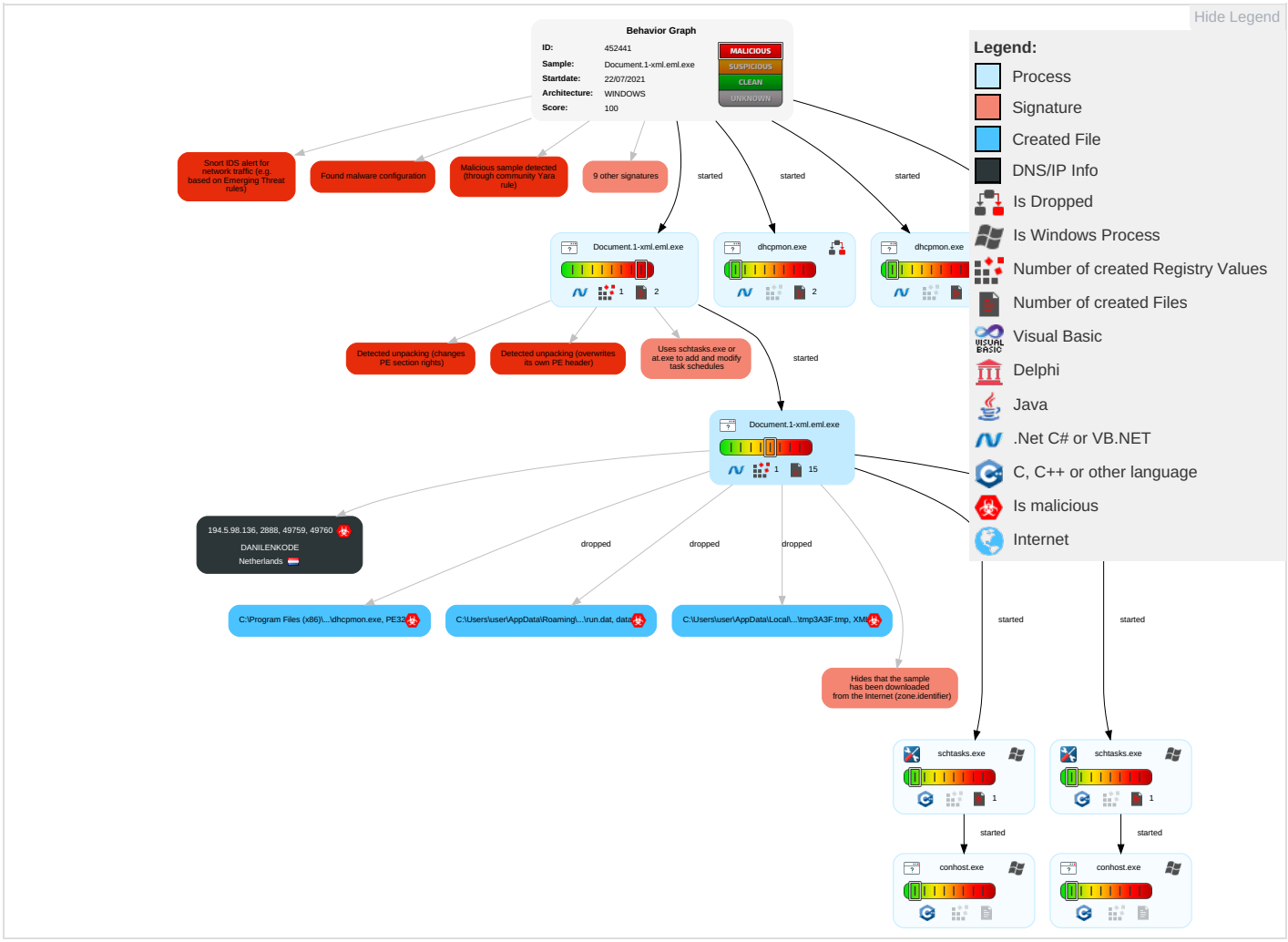
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networl Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	System Time Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdı Insecure Networl Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 2	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirec Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track D Locatior
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM Car Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 1 2	LSA Secrets	Account Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1	Manipul Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1 1	Cached Domain Credentials	System Owner/User Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial c Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 3	Proc Filesystem	System Information Discovery 4	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecure Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 3 3	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base St

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
Document.1-xml.eml.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoBot	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
15.2.Document.1-xml.eml.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.1.Document.1-xml.eml.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.Document.1-xml.eml.exe.52f0000.8.unpack	100%	Avira	TR/NanoCore.fadte		Download File
15.2.Document.1-xml.eml.exe.36e7a58.3.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
194.5.98.136	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
194.5.98.136	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.136	unknown	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452441
Start date:	22.07.2021
Start time:	11:09:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Document.1-xml.eml.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:	26
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@11/7@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.2% (good quality ratio 5.5%) • Quality average: 65.2% • Quality standard deviation: 31.4%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
11:11:10	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
11:11:11	API Interceptor	367x Sleep call for process: Document.1-xml.eml.exe modified
11:11:12	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Document.1-xml.eml.exe" s>$(Arg0)
11:11:13	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.136	hiSgJfiWKR.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	2 (P-O DRAWINGS) SUPPLY PRODUCT.exe	Get hash	malicious	Browse	• 194.5.98.212
	ynFBVCYIcu.exe	Get hash	malicious	Browse	• 194.5.98.195
	#RFQ ORDER7678432213211.exe	Get hash	malicious	Browse	• 194.5.98.120
	ORDER.exe	Get hash	malicious	Browse	• 194.5.98.23
	Q_007880.exe	Get hash	malicious	Browse	• 194.5.97.168
	eQqnH61qiB.exe	Get hash	malicious	Browse	• 194.5.98.207
	B32E407DC3284184684B29FD5235CBEDF2B60F60AED84.exe	Get hash	malicious	Browse	• 194.5.98.15
	MbBw6XTmif.exe	Get hash	malicious	Browse	• 194.5.98.107
	Jose Luis Ezeiza.cv7-15-2021.exe	Get hash	malicious	Browse	• 194.5.98.8
	t3uss3bjUL.exe	Get hash	malicious	Browse	• 194.5.98.182
	Agree Ment Letter-34222876190544.exe	Get hash	malicious	Browse	• 194.5.98.63
	purestub.exe	Get hash	malicious	Browse	• 194.5.98.63
	RFQ41000034331899945 65.exe	Get hash	malicious	Browse	• 194.5.98.195
	Order0045439090.exe	Get hash	malicious	Browse	• 194.5.98.8
	TPJCc3cswr.exe	Get hash	malicious	Browse	• 194.5.97.44
	Proof of payment.exe	Get hash	malicious	Browse	• 194.5.97.181
	Payment Schedule.xlsx	Get hash	malicious	Browse	• 194.5.97.44
	FbJ8HGm3HU.exe	Get hash	malicious	Browse	• 194.5.98.210
	sRXwLQjycE.exe	Get hash	malicious	Browse	• 194.5.98.107
	elmPEd3zO7.exe	Get hash	malicious	Browse	• 194.5.97.131

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\Document.1-xml.eml.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	266240
Entropy (8bit):	7.69767681098034
Encrypted:	false
SSDEEP:	6144:ql3N9PSj4kLkfPYD/z+gw/MyxSGsjB3ERuGDKI0nDzvQbBxSxg9eDxjXTWOA/uu:SN9PSjvLEwDLfKR9I3EzeIEqBxSxg9e0
MD5:	4D48E3CBFC19B5729B6C7A968A957805
SHA1:	4863E913B2E5709D9ED8C5937AE046E2EDEEE152
SHA-256:	45CF5D850CA6806FD9B55EF35A2EBE8AA2D9B724B67F96EAC270C44D1A85E810
SHA-512:	D77C98A1A9A15C4BBD63ED573043634D6AF46955ABAD40446A22B78F0B821445C63D6EA02A604A0388D6ADBE460C8BA8178D9AF8E3735DDE3AC28F3435E269 2
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L....q.^.....2.....z.....@..... .....l.....@.....8.....H... .....text..... ..`.rdata..B.....@..@.data.....l.....@....tineh.....p.....n.....@....rsrc.....p.....@..@..... ....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Document.1-xml.eml.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:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Temp\tmp3A3F.tmp	
Process:	C:\Users\user\Desktop\Document.1-xml.eml.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.103875449395091
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0YH5xtn:cbk4oL600QydbQxIYODOLedq3z5j
MD5:	F02D946FE2EDA095757A14A5D6B3BF6C
SHA1:	2AFBD7F5FBE2CA13357D9BE3DCAAF5F7162D32D4
SHA-256:	2BF693A2ADB49A20EE00B31714B8E284F8FE4090D4CEC038AC799DE677B91C03
SHA-512:	1BF8922586AEAD0DF782E6512FF8E80E952FA4895CA01991C0D8BD033E3B15F8D79D4C9DA7BD6A558540FE826D84280A5D3E0400599A37C0AA4970993C1F504
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 />.. <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\tmp3DCA.tmp	
Process:	C:\Users\user\Desktop\Document.1-xml.eml.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
Reputation:	moderate, very likely benign file
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\Document.1-xml.eml.exe
File Type:	data
Category:	modified
Size (bytes):	1624
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC08
MD5:	0D79388CEC6619D612C2088173BB6741
SHA1:	8A312E3198009C545D0CF3254572189D29A03EA7
SHA-256:	D7D423B23D932E306F3CCB2F7A984B7036A042C007A43FD655C6B57B960BB8DF
SHA-512:	53BB3E9263DFD746E7E8159466E220E6EC9D81E9D3F0E1D191E09CD511B7EB93B0BA65D13CE0C97C652ECD0F69BB991E6B1840F961BC65003C4DD7AA93EED13
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Document.1-xml.eml.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Ho:Ho
MD5:	74D4095194671D1DA20222ADFA1C18BC
SHA1:	4B47B8408E276625224DE42E215599003B266077
SHA-256:	3244CA869DD5C5746ACA3A8B6BD25780FE44BCD7AC82256D9DC93F42FDEE325A
SHA-512:	DC6C9A8BEA613BB3EC1CD9E123647EEB86587D9B6C20E25458F4D0EC2BB7FA6A81EF8209464E799CC8E500C96BE36C96D5E596C9C64139649567750BAE1870C
Malicious:	**true**
Preview:	..O..L.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Document.1-xml.eml.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.160383163865372
Encrypted:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
SSDEEP:	3:oNt+WfWhKH9lPy7L4A:oNwvcd5yPN
MD5:	B6A68884FD59FC6156B731FD07370D3F
SHA1:	287D7FE38B4353680C61C163FF0FD407CA5D9161
SHA-256:	EB08A56415072B846D03AECB1A5FD7B9570F90F79F92D6C7DDD37ACFBF28ED19
SHA-512:	DBCFCC356E58E3DDB3679010BB4F3CEC3AF3AF0608E87E2008AF75A0B0D50832E9A8BF1BDF66C7973A5A91C28C82618E7C8CF5250A2EC570DF8874193F8A185
Malicious:	false
Preview:	C:\Users\user\Desktop\Document.1-xml.eml.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.69767681098034
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.96% • Clipper DOS Executable (2020/12) 0.01% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Document.1-xml.eml.exe
File size:	266240
MD5:	4d48e3cbfc19b5729b6c7a968a957805
SHA1:	4863e913b2e5709d9ed8c5937ae046e2edeee152
SHA256:	45cf5d850ca6806fd9b55ef35a2ebe8aa2d9b724b67f96eac270c44d1a85e810
SHA512:	d77c98a1a9a15c4bbd63ed573043634d6af46955abad40446a22b78f0b821445c63d6ea02a604a0388d6adbe460c8ba8178d9af8e3735dde3ac28f3435e269c2
SSDEEP:	6144:ql3N9PSj4kLkfPYD/z+gw/MyxSGsjB3ERuGDKI0nDzvQbBxSxg9eDxjXTWOA/uu:SN9PSjvLEwDLfKR9I3EzeIEqBxSxg9e0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....q.^...

File Icon

Icon Hash:	cca6dacac2cacac0

Static PE Info

General

Entrypoint:	0x42e87a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x5EF671D4 [Fri Jun 26 22:08:20 2020 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5

General

Subsystem Version Minor:	0
Import Hash:	7bd0dc6ab22820cf89df2f4bb39531c5

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2d90b	0x2da00	False	0.975037457192	data	7.96899648432	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2f000	0x8d42	0x8e00	False	0.370956205986	data	6.01002219617	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x38000	0xedd0	0x200	False	0.35546875	data	3.0016604882	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tineh	0x47000	0xa	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x48000	0x9f88	0xa000	False	0.603100585938	data	6.13590130558	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	
FYRO Macedonia	Macedonia	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-11:11:12.962722	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	2888	192.168.2.4	194.5.98.136
07/22/21-11:11:19.563619	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	2888	192.168.2.4	194.5.98.136
07/22/21-11:11:25.992162	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	2888	192.168.2.4	194.5.98.136
07/22/21-11:11:32.486124	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	2888	192.168.2.4	194.5.98.136
07/22/21-11:11:39.847669	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	2888	192.168.2.4	194.5.98.136
07/22/21-11:11:46.236718	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	2888	192.168.2.4	194.5.98.136
07/22/21-11:11:53.077018	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	2888	192.168.2.4	194.5.98.136
07/22/21-11:11:59.559867	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49766	2888	192.168.2.4	194.5.98.136

Network Port Distribution

TCP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Document.1-xml.eml.exe PID: 6608 Parent PID: 5856

General

Start time:	11:09:54
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Document.1-xml.eml.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Document.1-xml.eml.exe'
Imagebase:	0x400000
File size:	266240 bytes
MD5 hash:	4D48E3CBFC19B5729B6C7A968A957805
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: 00000000.00000002.799147726.0000000000590000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.799147726.0000000000590000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.799147726.0000000000590000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: Document.1-xml.eml.exe PID: 5768 Parent PID: 6608

General

Start time:	11:11:08
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Document.1-xml.eml.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Document.1-xml.eml.exe'
Imagebase:	0x400000
File size:	266240 bytes
MD5 hash:	4D48E3CBFC19B5729B6C7A968A957805
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: 0000000F.00000002.925419136.00000000052F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.925419136.00000000052F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.925419136.00000000052F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000001.798397653.0000000000402000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000001.798397653.0000000000402000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000001.798397653.0000000000402000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.924630766.00000000036DF000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.917015310.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.917015310.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.917015310.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.925370927.0000000005050000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.925370927.0000000005050000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

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: 5796 Parent PID: 5768

General

Start time:	11:11:10
Start date:	22/07/2021

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\tmp3A3F.tmp'
Imagebase:	0x260000
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: 5960 Parent PID: 5796

General

Start time:	11:11:10
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5720 Parent PID: 5768

General

Start time:	11:11:11
Start date:	22/07/2021
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\tmp3DCA.tmp'
Imagebase:	0x260000
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: 5288 Parent PID: 5720

General

Start time:	11:11:11
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Document.1-xml.eml.exe PID: 5540 Parent PID: 968

General

Start time:	11:11:12
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\Document.1-xml.eml.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Document.1-xml.eml.exe 0
Imagebase:	0x400000
File size:	266240 bytes
MD5 hash:	4D48E3CBFC19B5729B6C7A968A957805
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 5556 Parent PID: 968

General

Start time:	11:11:13
Start date:	22/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x400000
File size:	266240 bytes
MD5 hash:	4D48E3CBFC19B5729B6C7A968A957805
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 20%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: dhcpmon.exe PID: 5608 Parent PID: 3424

General

Start time:	11:11:19
Start date:	22/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x400000
File size:	266240 bytes
MD5 hash:	4D48E3CBFC19B5729B6C7A968A957805
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: 00000017.00000002.920655306.0000000004A30000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000017.00000002.920655306.0000000004A30000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000017.00000002.920655306.0000000004A30000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis