ID: 528392
Sample Name: PO#042.exe
Cookbook: default.jbs
Time: 08:12:29
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

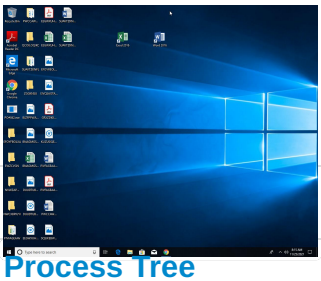
Windows Analysis Report PO#042.exe

Overview

General Information

Sample Name:	PO#042.exe
Analysis ID:	528392
MD5:	081ec29dd4df813.
SHA1:	a41a3e4874f2ded.
SHA256:	d9aa3e1081c430..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

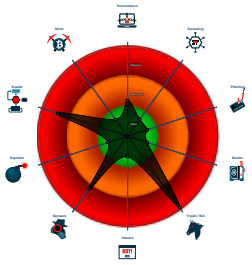
Nanocore AveMaria MailPassView

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

Signatures

- Found malware configuration
- Yara detected MailPassView
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Yara detected AveMaria stealer
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- PO#042.exe (PID: 7120 cmdline: "C:\Users\user\Desktop\PO#042.exe" MD5: 081EC29DD4DF8134F1F0C51F5620DD1A)
  - schtasks.exe (PID: 6516 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qCsCiBEHcy" /XML "C:\Users\user\AppData\Local\Temp\tmp5821.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6528 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PO#042.exe (PID: 6576 cmdline: {path} MD5: 081EC29DD4DF8134F1F0C51F5620DD1A)
    - schtasks.exe (PID: 6488 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpE454.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- PO#042.exe (PID: 6708 cmdline: C:\Users\user\Desktop\PO#042.exe 0 MD5: 081EC29DD4DF8134F1F0C51F5620DD1A)
  - schtasks.exe (PID: 3576 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qCsCiBEHcy" /XML "C:\Users\user\AppData\Local\Temp\tmp82EA.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3672 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - PO#042.exe (PID: 5768 cmdline: {path} MD5: 081EC29DD4DF8134F1F0C51F5620DD1A)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "15c24b29-1f3d-4f9d-946e-af4f83ba",
  "Group": "Blaze",
  "Domain1": "rickjohssn.ddns.net",
  "Domain2": "",
  "Port": 5612,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "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
00000011.00000002.341913940.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000011.00000002.341913940.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000011.00000002.341913940.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000011.00000000.326594390.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000011.00000000.326594390.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 74 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.PO#042.exe.5700000.13.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
11.2.PO#042.exe.5700000.13.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
17.0.PO#042.exe.400000.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
17.0.PO#042.exe.400000.12.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
17.0.PO#042.exe.400000.12.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 160 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

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 submitted file

Yara detected AveMaria stealer

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected AveMaria stealer

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

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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 MailPassView

Yara detected AveMaria stealer

Yara detected Nanocore RAT

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected Nanocore Rat

Yara detected AveMaria stealer

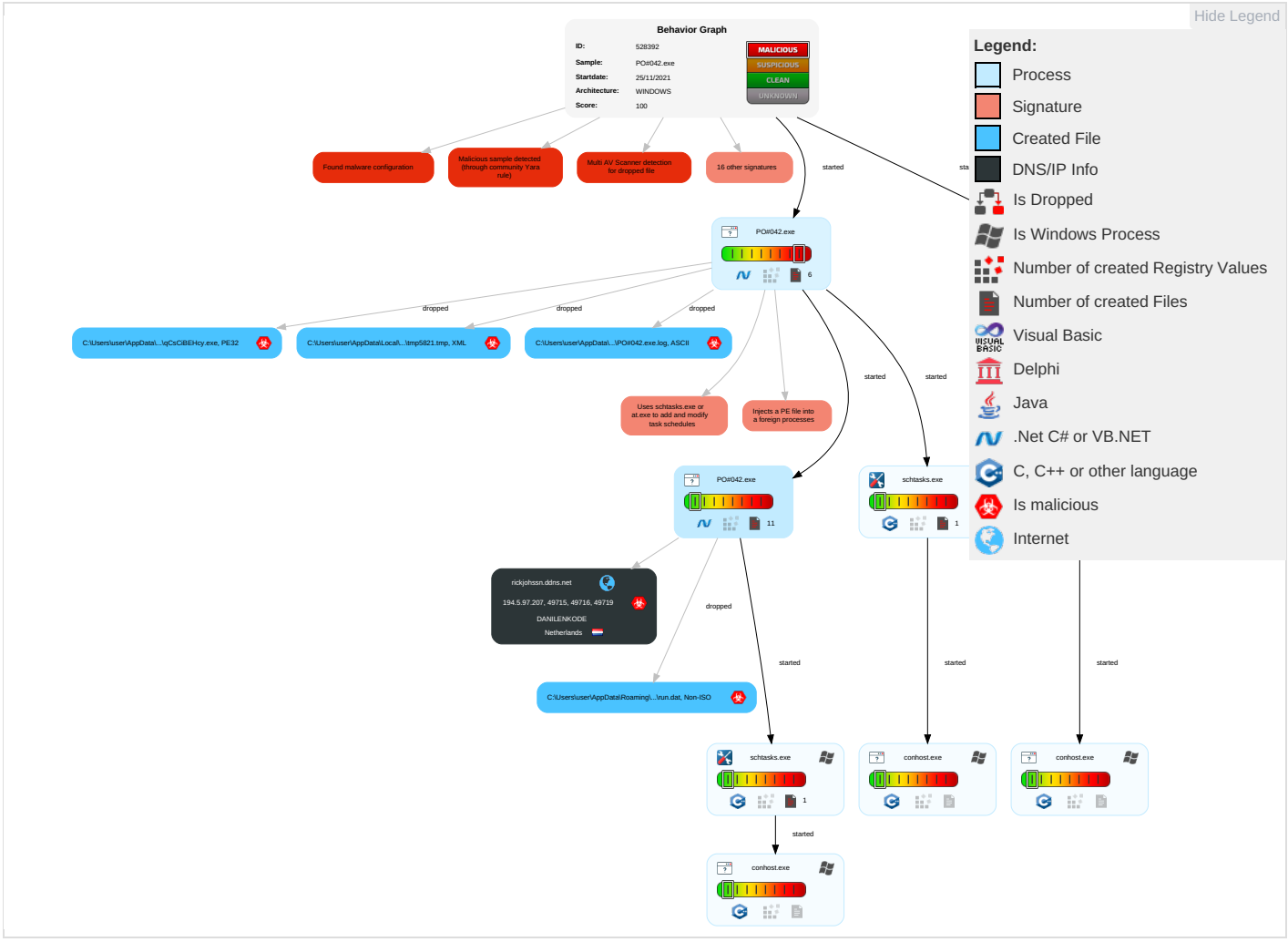
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	E I N C

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 1	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	D I F

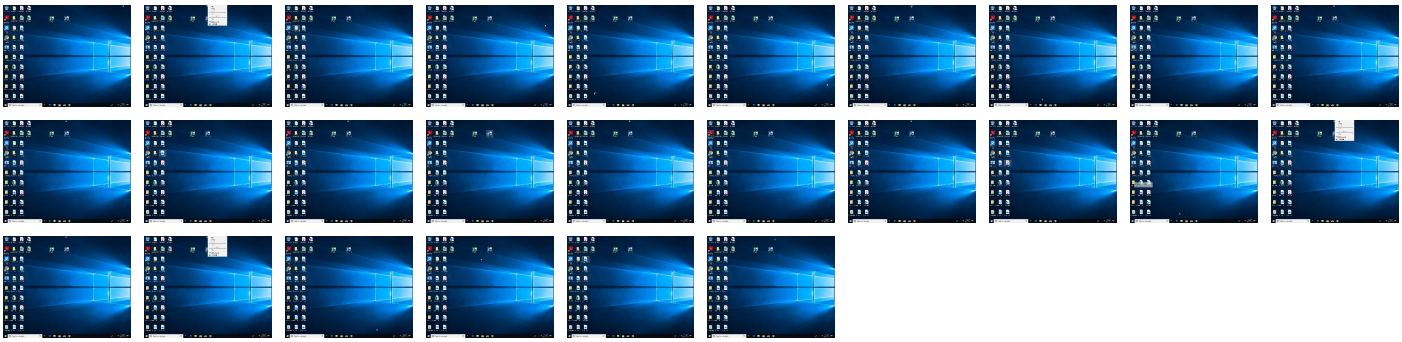
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PO#042.exe	25%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	
PO#042.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\qCsCiBEHcy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\qCsCiBEHcy.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.PO#042.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.PO#042.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.PO#042.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.PO#042.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.PO#042.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.PO#042.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.PO#042.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.PO#042.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.PO#042.exe.5ab0000.15.unpack	100%	Avira	TR/NanoCore.fadte		Download File
11.0.PO#042.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.PO#042.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.PO#042.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.PO#042.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
rickjohssn.ddns.net	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.comn-u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/tali	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnI	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fontbureau.comdia	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/den	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sajatypeworks.come	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/S	0%	URL Reputation	safe	
http://www.tiro.comslnt	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.tiro.comt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/sl-s	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/J	0%	URL Reputation	safe	
http://www.carterandcone.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/v	0%	URL Reputation	safe	
http://www.carterandcone.comn	0%	URL Reputation	safe	
rickjohssn.ddns.net	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comm	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/u	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/0_	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/o	0%	URL Reputation	safe	
http://www.sajatypeworks.comQx	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcea	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/d	0%	URL Reputation	safe	
http://www.tiro.comh	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rickjohssn.ddns.net	194.5.97.207	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
rickjohssn.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.207	rickjohssn.ddns.net	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528392
Start date:	25.11.2021
Start time:	08:12:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO#042.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:	31
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.spyw.evad.winEXE@15/10@15/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.6% (good quality ratio 0.6%) • Quality average: 67.7% • Quality standard deviation: 14.2%
HCA Information:	• Successful, ratio: 98% • 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
08:13:27	API Interceptor	2x Sleep call for process: PO#042.exe modified
08:13:35	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\PO#042.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.207	RzUbulerbF.exe	Get hash	malicious	Browse	
	NOA MU21S0029729.exe	Get hash	malicious	Browse	
	SK202-8 #YN12-60387.exe	Get hash	malicious	Browse	
	a34b93ef-dea2-45f8-a5bf-4f6b0b5291c7.exe	Get hash	malicious	Browse	
	3fcd8c19-af88-4cd9-87e7-0bfea1de01a1.exe	Get hash	malicious	Browse	
	5zLV4brBQ7.exe	Get hash	malicious	Browse	
	Bank Information.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	Original Bill of Lading_xls.exe	Get hash	malicious	Browse	• 194.5.97.128
	NEUE BESTELLUNG 132542,pdf.exe	Get hash	malicious	Browse	• 194.5.97.23
	Purchase Order.exe	Get hash	malicious	Browse	• 194.5.97.210
	PURCHASE ORDER EXPORT1024MG97364032 SCANNED DOC_pdf.exe	Get hash	malicious	Browse	• 194.5.98.48
	purchase order Nl32855 (1).exe	Get hash	malicious	Browse	• 194.5.98.139
	8mTwU7uNFV.exe	Get hash	malicious	Browse	• 194.5.97.131
	KNpmkMT5f3.exe	Get hash	malicious	Browse	• 194.5.98.12
	scvRj4lo1E.exe	Get hash	malicious	Browse	• 194.5.98.11
	#RFQ ORDER484425083-NJ.exe	Get hash	malicious	Browse	• 194.5.98.120
	RzUbulerbF.exe	Get hash	malicious	Browse	• 194.5.97.207
	SIGNED_COPY_IMG_ORDER_...REQUEST_IMG_123456.exe	Get hash	malicious	Browse	• 194.5.98.5

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NOA MU21S0029729.exe	Get hash	malicious	Browse	• 194.5.97.207
	New purchase order 4940009190,pdf.exe	Get hash	malicious	Browse	• 194.5.97.23
	Fattura_del_cliente_V406307-scan.exe	Get hash	malicious	Browse	• 194.5.97.165
	ML822VOG-R11.doc	Get hash	malicious	Browse	• 194.5.97.131
	6Xzgfme0z6.exe	Get hash	malicious	Browse	• 194.5.97.131
	ESTADO+10+DE+NOVIEMBRE+DE+2021-101121.pdf.js	Get hash	malicious	Browse	• 194.5.98.48
	RTQFHtPW9x.exe	Get hash	malicious	Browse	• 194.5.98.107
	Document#053681.exe	Get hash	malicious	Browse	• 194.5.98.204
	4vo6jE1nlG.exe	Get hash	malicious	Browse	• 194.5.97.54

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\PO#042.exe.log

Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, 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\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\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp5821.tmp

Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.1926346339507825
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3tn:cbh47TlNQ//rydbz9l3YODOLNdq37
MD5:	BC9DDCAFECB58D40C63482034EAAE2AF
SHA1:	131776F663E55D39485741E3035EE8F38F74B65F
SHA-256:	698B96E1DBB7D6C1B6531750D43BBDCEB0638CEA37F6CFCC3EFC9878C769F5A7
SHA-512:	02A61BB90F0F748D118B9254BDCE6029C01B1DB59581921CD65BFB37DB4F1127F4DFBD93564CC289F238312C7678F070FDB0055241528BF61C1DC41A552FD8D
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\tmp82EA.tmp

Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\tmp82EA.tmp

Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.1926346339507825
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3tn:cbh47TlNQ//rydbz9l3YODOLNdq37
MD5:	BC9DDCAFECB58D40C63482034EAAE2AF
SHA1:	131776F663E55D39485741E3035EE8F38F74B65F
SHA-256:	698B96E1DBB7D6C1B6531750D43BBDCEB0638CEA37F6CFCC3EFC9878C769F5A7
SHA-512:	02A61BB90F0F748D118B9254BDCE6029C01B1DB59581921CD65BFB37DB4F1127F4DFBD93564CC289F238312C7678F070FDB0055241528BF61C1DC41A552FD8D
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\tmpE454.tmp

Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1296
Entropy (8bit):	5.109973900909971
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0j8xtn:cbk4oL600QydbQxlYODOLedq3W8j
MD5:	4F1801BE0F2561BC7A685C90F44B571A
SHA1:	E9BC36FE56E489EBAD5C03FA84E43C4FFCD6AFF5
SHA-256:	CEA799752CC5190FD0C0A5138C56CC9ADFDFAD966C05E8AEEAE865EADEC8F6F0
SHA-512:	EE4CCF6BF2CBFEEB5D409513C241E2DB7B90EAC7EF7F55BD63F923B9739A0A02E721ED8D48125A9EA3EAD49F65695D7A87968882CD46BAD491D6F99732D42193
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\PO#042.exe
File Type:	data
Category:	dropped
Size (bytes):	128
Entropy (8bit):	6.527114648336088
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRH5/ljRAaTlKYrI1Sj9txROIsxcMek2:X4LDAn1rplKTYBROIsxek2
MD5:	0A9C5EAE8756D6FC90F59D8D71A79E1E
SHA1:	0F7D6AAED17CD18DC614535ED26335C147E29ED7
SHA-256:	B1921EA14C66927397BAF3FA456C22B93C30C3DE23546087C0B18551CE5001C5
SHA-512:	78C2F399AC49C78D89915DFF99AC955B5E0AB07BAAD61B07B0CE073C88C1D3A9F1D302C2413691B349DD34441B0FF909C08A4F71E2F1B73F46C1FF308BC7CFA
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P.OT....g.t....'7.....)..8zII..K/....n3...3.5.....&.7].)..wL...:}g...@...mV.....JUP...w

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

Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:PiLq:aLq

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
MD5:	BCC68C34BF7F957C15E590FA3E88242F
SHA1:	FD65CAE12EF03CDE4ECE60562608A99F9588D600
SHA-256:	D60E408E5A510870813F09E7F9A5C62D0B4F6C0B15C016C8AC78C8EB896DA1C3
SHA-512:	A6378EF4B54598249B39DC58D2AE364C53C3FDA287A7F0D86B40F80A61299649F9E8A5B307C4456B1E684B639344F9C21A7094A48DE5857FBD25D30B60936A88
Malicious:	**true**
Preview:	z.2....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	data
Category:	dropped
Size (bytes):	367496
Entropy (8bit):	**7.999535722214108**
Encrypted:	**true**
SSDEEP:	6144:3rv1Xjouu5ZMQajChQSE0Rp30gbdoh5Y2cmSPCqA9BCNHku9BdFqB3GbiCX:D1TousJSafd6imJd8EeBdF7biCX
MD5:	4D784935677AE26ACDC3FB84FA1E6CF8
SHA1:	4B143D26638C2BE44BE05D862E5CD1BEA3664825
SHA-256:	C77E2D82DB9066E4DBFDE3AE0461A4259505F435EC0DB2CE3BD005BE0E2DE67C
SHA-512:	193295AB3FBCE6BA4A563DD864839F5D7A3B8F351F576DE2C85E2F3978F3E33EF22299224DFD7D2F5506A2CAFB04656E19676F28B21F19C504B2D43921063554
Malicious:	false
Preview:	..m.....%.8C.....o`.M..d....mvW5].N ...c....m.b..1^J@....M.!.aq.f....<....._..;i.1-+.wZ..C@Z...> .P9.K..[~....1.....#.Djp...q..z..HoR/..8....k.....\.7..c..]_.....F.....3Z.9U.....r.. 8..]..%n..Q..^<s`L{. ..9.o..wU33z...hJG..!..a.?mI...}.H}...o.Zs`.....~..x....".7.{....k.>. @X.\j.....57..C..f.v...:..Q<.B.o..x..s}\.`....z..E@$.!.}}.&.VI.....Y.....gU..b.b..I..Bg....bh .$.....f.B...e.f...a.....v.....9..x.#.....*[.....=.T#.,.6.uN.....D.jdQ..go.T..+..N.U-.w.a..6 C.5.vMy....S...V...I...:..v2..V.....G..P K.{.&.....o...q.....`~.i8.....+k.F...o.$TP.... I.....;T..3.a.u.f..)...4b...-.r.&(<....'....n.[...b....k....W.Vp..G`..~...''k....Y../l3`....u_.L...#.....;....m.cV.|.:.....#..P9;....Q..*F._%.f..0...'.z.i..#;.X=.utJ...)9".....k..E..K...\..cc-..8<..f.T!{ ..c....S`4{....D2..s.....)`.h.;.QQ^mP.M77.'M.....q C).I....<..]QA.,...p.....4..XQ.xu.w.z..g~.%M.....D...!.h.F.$~.....n%'.lt..E...h=.....).?.....N.K?.M.48..

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	33
Entropy (8bit):	4.35485207383835
Encrypted:	false
SSDEEP:	3:oNWXp5v1qC4An:oNWXpFgC4An
MD5:	14FF4FB46A04E960CC58BA22CB62A191
SHA1:	C586A0EFD442B6D00FC49C2E225EDF9170A3D3A1
SHA-256:	371038D01254CF846F9B88263579B6B1808152C154CA42ED436F8831DAB8E971
SHA-512:	1FEB71C24BDAEEF54DC5C4BF9D627CA4F31C05AF52E1153F458DB8C068FDCE47057169E947322879CC1875AF4DD33892958F954D9DFA20B84273C5B47FC00F 3
Malicious:	false
Preview:	C:\Users\user\Desktop\PO#042.exe

C:\Users\user\AppData\Roaming\qCsCiBEHcy.exe	
Process:	C:\Users\user\Desktop\PO#042.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	441344

C:\Users\user\AppData\Roaming\qCsCiBEHcy.exe	
Entropy (8bit):	7.961902355627955
Encrypted:	false
SSDEEP:	12288:zZYWUs9aNUDmR+SDZdzVbC0cy4d5cwXEzXtfya3:NDU+dm4ozVbClLd5rXgMa3
MD5:	081EC29DD4DF8134F1F0C51F5620DD1A
SHA1:	A41A3E4874F2DEDCC28A732F12C2A9E0EFC84995
SHA-256:	D9AA3E1081C4300AB2C24DF237E2CE1F3D66E0C1B8856A2A01D5B95449DCCF58
SHA-512:	218A57098C4F3069158C3F9340803BF344D16862F1ED91A74CC4CC62EF77B1A9DD9FDEAF37973677622D8F81393048C7A340EDDF6B2F90C7C7539223E29E4564
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....@.. ....@.....W..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....9.....j...dQ..lE.....z.(.....}.....(....o....}....*..0.....{.....3.....(....*.....0.....{.....,....f.....}..... }.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(.....*.....n..}.....{... .,..{....oh...*..{....*.s..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.961902355627955
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	PO#042.exe
File size:	441344
MD5:	081ec29dd4df8134f1f0c51f5620dd1a
SHA1:	a41a3e4874f2dedcc28a732f12c2a9e0efc84995
SHA256:	d9aa3e1081c4300ab2c24df237e2ce1f3d66e0c1b8856a2a01d5b95449dccf58
SHA512:	218a57098c4f3069158c3f9340803bf344d16862f1ed91a74cc4cc62ef77b1a9dd9fdeaf37973677622d8f81393048c7a340eddf6b2f90c7c7539223e29e4564
SSDEEP:	12288:zZYWUs9aNUDmR+SDZdzVbC0cy4d5cwXEzXtfya3:NDU+dm4ozVbClLd5rXgMa3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a..... .....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46d0de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619F149C [Thu Nov 25 04:44:12 2021 UTC]
TLS Callbacks:	

General

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

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6b0e4	0x6b200	False	0.967405374854	data	7.96966577385	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x580	0x600	False	0.421223958333	data	4.45517854682	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-08:13:37.483234	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52806	8.8.8.8	192.168.2.3
11/25/21-08:13:44.167242	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53910	8.8.8.8	192.168.2.3
11/25/21-08:13:50.712939	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60784	8.8.8.8	192.168.2.3
11/25/21-08:13:56.812547	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51143	8.8.8.8	192.168.2.3

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 08:13:37.462006092 CET	192.168.2.3	8.8.8.8	0x394b	Standard query (0)	rickjohssn.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:13:44.144660950 CET	192.168.2.3	8.8.8.8	0x716d	Standard query (0)	rickjohssn.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:13:50.691493034 CET	192.168.2.3	8.8.8.8	0xeff5	Standard query (0)	rickjohssn.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:13:56.790839911 CET	192.168.2.3	8.8.8.8	0x975d	Standard query (0)	rickjohssn.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 08:14:02.647743940 CET	192.168.2.3	8.8.8.8	0xdffe	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:09.630845070 CET	192.168.2.3	8.8.8.8	0x27b9	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:16.508111954 CET	192.168.2.3	8.8.8.8	0xefb6	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:22.335279942 CET	192.168.2.3	8.8.8.8	0x9963	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:28.067934036 CET	192.168.2.3	8.8.8.8	0x7366	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:34.565203905 CET	192.168.2.3	8.8.8.8	0x6660	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:41.381736994 CET	192.168.2.3	8.8.8.8	0x725a	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:47.116056919 CET	192.168.2.3	8.8.8.8	0x134	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:53.009850025 CET	192.168.2.3	8.8.8.8	0xfe7d	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:58.762325048 CET	192.168.2.3	8.8.8.8	0x48d8	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 08:15:05.371923923 CET	192.168.2.3	8.8.8.8	0x2979	Standard query (0)	rickjohssn .ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 08:13:37.483233929 CET	8.8.8.8	192.168.2.3	0x394b	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:13:44.167242050 CET	8.8.8.8	192.168.2.3	0x716d	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:13:50.712939024 CET	8.8.8.8	192.168.2.3	0xeff5	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:13:56.812546968 CET	8.8.8.8	192.168.2.3	0x975d	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:02.667552948 CET	8.8.8.8	192.168.2.3	0xdffe	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:09.650866032 CET	8.8.8.8	192.168.2.3	0x27b9	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:16.527796984 CET	8.8.8.8	192.168.2.3	0xefb6	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:22.354964018 CET	8.8.8.8	192.168.2.3	0x9963	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:28.085798025 CET	8.8.8.8	192.168.2.3	0x7366	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:34.585793972 CET	8.8.8.8	192.168.2.3	0x6660	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:41.401089907 CET	8.8.8.8	192.168.2.3	0x725a	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:47.137159109 CET	8.8.8.8	192.168.2.3	0x134	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:53.030652046 CET	8.8.8.8	192.168.2.3	0xfe7d	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:14:58.781963110 CET	8.8.8.8	192.168.2.3	0x48d8	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)
Nov 25, 2021 08:15:05.392036915 CET	8.8.8.8	192.168.2.3	0x2979	No error (0)	rickjohssn .ddns.net		194.5.97.207	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: PO#042.exe PID: 7120 Parent PID: 4864

General

Start time:	08:13:21
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\PO#042.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\PO#042.exe"
Imagebase:	0xce0000
File size:	441344 bytes
MD5 hash:	081EC29DD4DF8134F1F0C51F5620DD1A
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: 00000001.00000002.305672479.0000000004331000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.305672479.0000000004331000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.305672479.0000000004331000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6516 Parent PID: 7120

General

Start time:	08:13:29
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qCsCiBEHcy" /XML "C:\Users\user\AppData\Local\Temp\tmp5821.tmp
Imagebase:	0xb0000
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: 6528 Parent PID: 6516

General

Start time:	08:13:30
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: PO#042.exe PID: 6576 Parent PID: 7120

General

Start time:	08:13:30
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\PO#042.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8c0000
File size:	441344 bytes
MD5 hash:	081EC29DD4DF8134F1F0C51F5620DD1A
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: 0000000B.00000000.301904018.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.301904018.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.301904018.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.560554791.00000000064D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.560554791.00000000064D0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.560896197.0000000007131000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.553259676.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.553259676.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.553259676.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.303219427.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.303219427.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.303219427.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.560527009.00000000064C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.560527009.00000000064C0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.557454662.000000000312D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.557454662.000000000312D000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.560629867.0000000006510000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.560629867.0000000006510000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.559477519.0000000005AB0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.559477519.0000000005AB0000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.559477519.0000000005AB0000.00000004.00020000.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.302397117.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.302397117.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.302397117.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.558192518.00000000043BA000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.557801624.00000000040D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000B.00000002.557801624.00000000040D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_AveMaria, Description: Yara detected AveMaria stealer, Source: 0000000B.00000002.557801624.00000000040D1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000B.00000002.560816658.0000000006931000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.560312852.0000000006470000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.560312852.0000000006470000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.560217789.0000000006450000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.560217789.0000000006450000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.302780129.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.302780129.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.302780129.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.560367349.0000000006490000.00000004.00020000.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source:

	0000000B.00000002.560367349.0000000006490000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.559222634.0000000005700000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.559222634.0000000005700000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6488 Parent PID: 6576

General

Start time:	08:13:33
Start date:	25/11/2021
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\tmpE454.tmp
Imagebase:	0xb0000
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: 6400 Parent PID: 6488

General

Start time:	08:13:34
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: PO#042.exe PID: 6708 Parent PID: 664

General

Start time:	08:13:35
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\PO#042.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\PO#042.exe 0
Imagebase:	0xd90000
File size:	441344 bytes
MD5 hash:	081EC29DD4DF8134F1F0C51F5620DD1A
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: 0000000E.00000002.330166499.0000000004411000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.330166499.0000000004411000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.330166499.0000000004411000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3576 Parent PID: 6708

General

Start time:	08:13:40
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\qCsCiBEHcy" /XML "C:\Users\user\AppData\Local\Temp\tmp82EA.tmp
Imagebase:	0xb0000
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: 3672 Parent PID: 3576

General

Start time:	08:13:41
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: PO#042.exe PID: 5768 Parent PID: 6708

General

Start time:	08:13:42
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\PO#042.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x960000
File size:	441344 bytes
MD5 hash:	081EC29DD4DF8134F1F0C51F5620DD1A
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: 00000011.00000002.341913940.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.341913940.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.341913940.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.326594390.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.326594390.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.326594390.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.327764253.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.327764253.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.327764253.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.326127526.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.326127526.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.326127526.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.327281473.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.327281473.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.327281473.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.342636302.0000000003F71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.342636302.0000000003F71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.342567013.0000000002F71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.342567013.0000000002F71000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis