ID: 526911
Sample Name: Purchase Order.exe
Cookbook: default.jbs
Time: 07:43:08
Date: 23/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

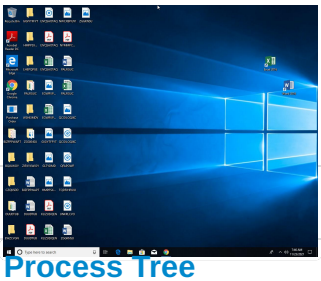
Windows Analysis Report Purchase Order.exe

Overview

General Information

Sample Name:	Purchase Order.exe
Analysis ID:	526911
MD5:	3f4e18fa2e1404e..
SHA1:	435587d7a9213b..
SHA256:	5a608e9daf5aca1.
Tags:	exe nanocore
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

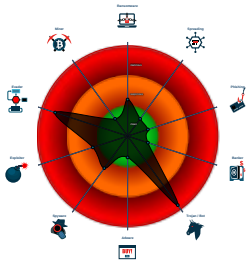
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- 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…
- Sigma detected: Suspicius Add Tas…

Classification



Process Tree

- **System is w10x64**
- Purchase Order.exe (PID: 4948 cmdline: "C:\Users\user\Desktop\Purchase Order.exe" MD5: 3F4E18FA2E1404E2C8F7F7E58C0DAE4E)
  - schtasks.exe (PID: 2940 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\sWTAwlQUDpm" /XML "C:\Users\user\AppData\Local\Temp\tmpFF67.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase Order.exe (PID: 2840 cmdline: {path} MD5: 3F4E18FA2E1404E2C8F7F7E58C0DAE4E)
    - schtasks.exe (PID: 4664 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp5DEB.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 5148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Purchase Order.exe (PID: 4576 cmdline: "C:\Users\user\Desktop\Purchase Order.exe" 0 MD5: 3F4E18FA2E1404E2C8F7F7E58C0DAE4E)
  - schtasks.exe (PID: 2960 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\sWTAwlQUDpm" /XML "C:\Users\user\AppData\Local\Temp\tmp2DF9.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase Order.exe (PID: 5872 cmdline: {path} MD5: 3F4E18FA2E1404E2C8F7F7E58C0DAE4E)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "97f187e8-a15c-4801-9810-760fe379",
  "Group": "Bllie",
  "Domain1": "billie4.ddns.net",
  "Domain2": "",
  "Port": 6272,
  "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
00000003.00000002.514093712.000000000445 1000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000000.290105146.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000000.290105146.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000E.00000000.290105146.000000000040 2000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000003.00000002.510612941.000000000140 0000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
Click to see the 71 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.Purchase Order.exe.5c30000.26.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
3.2.Purchase Order.exe.5c30000.26.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
3.2.Purchase Order.exe.3495c98.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
3.2.Purchase Order.exe.3495c98.12.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
14.0.Purchase Order.exe.400000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 185 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

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

.NET source code contains very large strings

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

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 Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

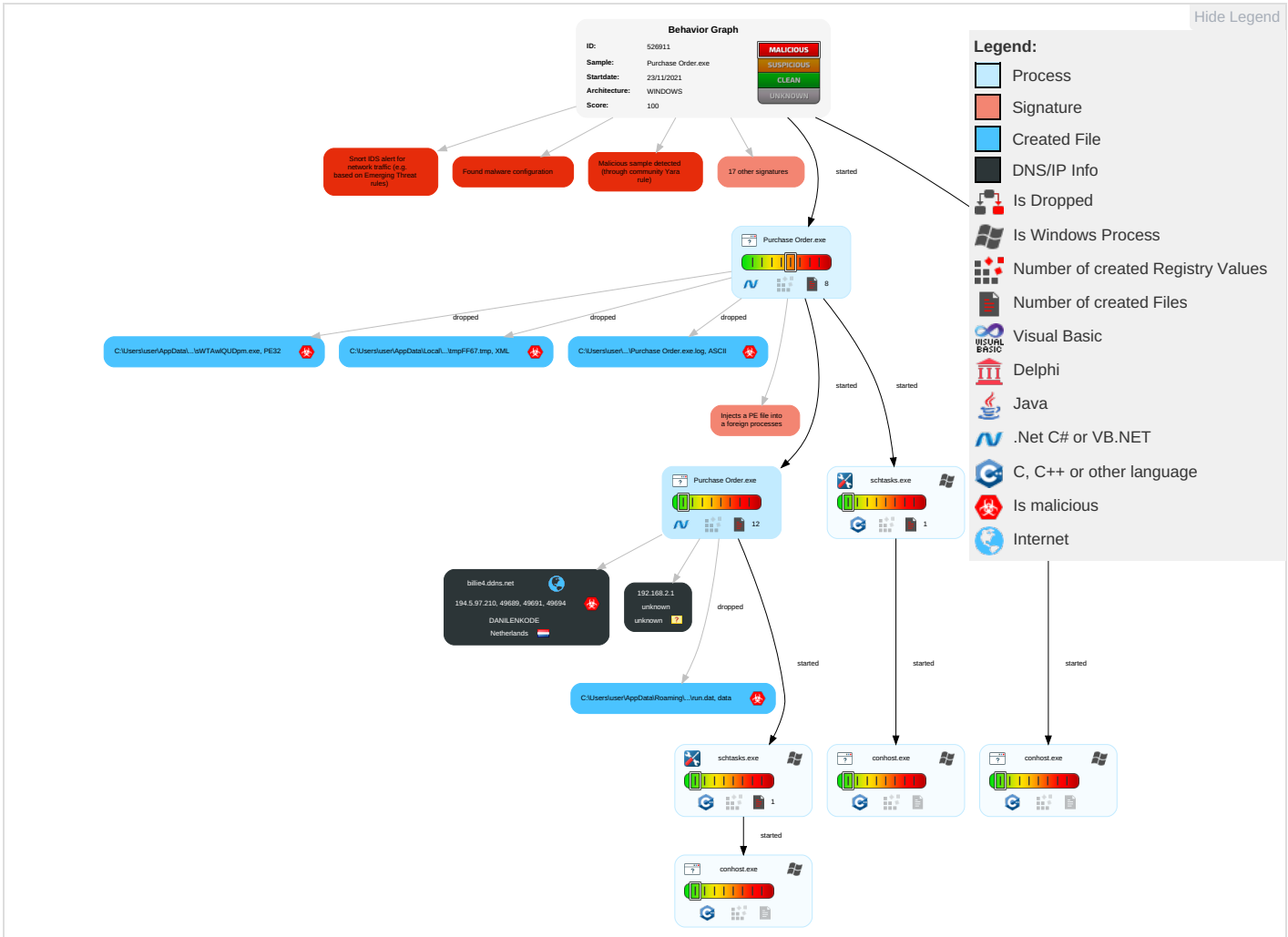
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit Redirec Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exploit Track D Locatio

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	System Information Discovery 1 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Security Software Discovery 2 1	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Layer Protocol 2 1	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 1	DCSync	Virtualization/Sandbox Evasion 2 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 1 1 2	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

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
Purchase Order.exe	11%	ReversingLabs	ByteCode-MSIL.Backdoor.Bladabhindi	
Purchase Order.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\sWTAwlQUDpm.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\sWTAwlQUDpm.exe	24%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
14.0.Purchase Order.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Purchase Order.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Purchase Order.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.Purchase Order.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.Purchase Order.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.Purchase Order.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.2.Purchase Order.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.Purchase Order.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.Purchase Order.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.Purchase Order.exe.5ff0000.29.unpack	100%	Avira	TR/NanoCore.fadte		Download File
3.0.Purchase Order.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Purchase Order.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
14.0.Purchase Order.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
billie4.ddns.net	2%	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.jiyu-kobo.co.jp/5qJ	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnL	0%	URL Reputation	safe	
http://www.sandoll.co.kr5	0%	Avira URL Cloud	safe	
http://www.sandoll.co.krttp://w	0%	Avira URL Cloud	safe	
http://www.tiro.comfr-cNqQ	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krNwS	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr.	0%	Avira URL Cloud	safe	
billie4.ddns.net	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0r	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com.	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/mq	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/lq.	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	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.jiyu-kobo.co.jp/5	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/b	0%	Avira URL Cloud	safe	
http://www.fontbureau.comFqw	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.kructv	0%	Avira URL Cloud	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	

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cnf	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comqw	0%	Avira URL Cloud	safe	
http://www.fontbureau.commno	0%	Avira URL Cloud	safe	
http://www.tiro.TqO	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnTF	0%	URL Reputation	safe	
http://www.sandoll.co.krw.micro	0%	Avira URL Cloud	safe	
http://en.wikipedia	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0t:	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	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/	0%	URL Reputation	safe	
http://www.fontbureau.comdjp/5qJ	0%	Avira URL Cloud	safe	
http://www.fontbureau.comitu	0%	URL Reputation	safe	
http://https://ocram-codes.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/vq	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueet5	0%	Avira URL Cloud	safe	
http://www.tiro.com3p	0%	Avira URL Cloud	safe	
http://www.goodfont.co.krlp	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr~v	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0-u	0%	Avira URL Cloud	safe	
http://www.carterandcone.comresnv	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
billie4.ddns.net	194.5.97.210	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
billie4.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.97.210	billie4.ddns.net	Netherlands		208476	DANILENKODE	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	526911
Start date:	23.11.2021
Start time:	07:43:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order.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:	25
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@15/10@20/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 97% • 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
07:44:07	API Interceptor	2x Sleep call for process: Purchase Order.exe modified
07:44:15	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Purchase Order.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.97.210	10377 APT800_B0205K0384.exe	Get hash	malicious	Browse	
	PO-10377.exe	Get hash	malicious	Browse	
	Purchase Order_PO226520_1632165053105.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	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
	RzUbuIerbF.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
	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
	ORDEN DE COMPRA-PDF.exe	Get hash	malicious	Browse	• 194.5.97.149
	Confirmation Transfer Copy MT102-Ref No#01018.exe	Get hash	malicious	Browse	• 194.5.98.105
	Confirmation Transfer Copy MT102-Ref No-01018.exe	Get hash	malicious	Browse	• 194.5.98.105

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Purchase Order.exe.log	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	916
Entropy (8bit):	5.282390836641403
Encrypted:	false
SSDEEP:	24:MLF20NaL3z2p29hJ5g522rW2xAi3AP26K95rKoO2+g2+:MwLLD2Y9h3go2rxxAcAO6ox+g2+
MD5:	5AD8E7ABEADADAC4CE06FF693476581A
SHA1:	81E42A97BBE3D7DE8B1E8B54C2B03C48594D761E
SHA-256:	BAA1A28262BA27D51C3A1FA7FB0811AD1128297ABB2EDCCC785DC52667D2A6FD
SHA-512:	7793E78E84AD36CE65B5B1C015364E340FB9110FAF199BC0234108CE9BCB1AEDACBD25C6A012AC99740E08BEA5E5C373A88E553E47016304D8AE6AEEAB58EEFF
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Configuration\de460308a9099237864d2ec2328fc958\System.Configuration.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp2DF9.tmp	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1648
Entropy (8bit):	5.172217402109266
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp2DF9.tmp	
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBNOtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3M
MD5:	0371FFF5870C0D59235E3FD3647E5538
SHA1:	358AA8B8346B514512F900E57C3204D77133DF2C
SHA-256:	C1AB5FE0B70B71F5B3890D43561AD435D9384E94293E7FB952E64414D6086A22
SHA-512:	DB0BD5EB36EBF58B883AD95657AA4BF552B2A5BAF6BE8B97719E8B6C85CCFA6DAB784E0798F54BBC8384128082FF009C91B2DE3A01ACC20CAE04711B76175267
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>t

C:\Users\user\AppData\Local\Temp\tmp5DEB.tmp	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1305
Entropy (8bit):	5.088117605128047
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0PbDxtn:cbk4oL600QydbQxIYODOLedq3SPj
MD5:	F8DE240D4239D85AB6315F533A21B115
SHA1:	CFE83B8E774B9949C0E068EC7746E857628025F9
SHA-256:	8CE0227F4A53D2BC6D1C17C6F2B4339A93A2200E386C7CD7FB85DB365E189DA1
SHA-512:	D6E8560D9D08DAD33961DED978DA40ECEB3B094AFD26283AF415A382604C916D00777D73F4F8F5CEE94B50E98261F5D37A1D873F676D04EF9E00282FAF9E3FA
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\Local\Temp\tmpFF67.tmp	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1648
Entropy (8bit):	5.172217402109266
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBNOtn:cbhC7ZlNQF/rydbz9I3YODOLNdq3M
MD5:	0371FFF5870C0D59235E3FD3647E5538
SHA1:	358AA8B8346B514512F900E57C3204D77133DF2C
SHA-256:	C1AB5FE0B70B71F5B3890D43561AD435D9384E94293E7FB952E64414D6086A22
SHA-512:	DB0BD5EB36EBF58B883AD95657AA4BF552B2A5BAF6BE8B97719E8B6C85CCFA6DAB784E0798F54BBC8384128082FF009C91B2DE3A01ACC20CAE04711B76175267
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>.. <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>t

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	data
Category:	dropped
Size (bytes):	128
Entropy (8bit):	6.527114648336088
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRH5/ljRAaTlKYrI1Sj9txROIsxcMek2:X4LDAn1rplKTYBROIsxek2
MD5:	0A9C5EAE8756D6FC90F59D8D71A79E1E

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
SHA1:	0F7D6AAED17CD18DC614535ED26335C147E29ED7
SHA-256:	B1921EA14C66927397BAF3FA456C22B93C30C3DE23546087C0B18551CE5001C5
SHA-512:	78C2F399AC49C78D89915DFF99AC955B5E0AB07BAAD61B07B0CE073C88C1D3A9F1D302C2413691B349DD34441B0FF909C08A4F71E2F1B73F46C1FF308BC7CF A
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\Purchase Order.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:0It:0Q
MD5:	BE3EB2224A65D1EC10EE8F55BA8B4CB1
SHA1:	1607DB06531CBA588752E844FB53B97A863FF4BD
SHA-256:	9C9D4D78A2F1EC733AEC21A6CB734BEE54C591D8F4E9A80C2994E62D8568AAE9
SHA-512:	572C92BBED9DC189D4CA39441F7482C56C86CD7EBEA110CE733368BB1EFC1E017F2ED2B54B90C910BA9A52620F3A571CFF5DC39224FD534530EA02230D5B1C B
Malicious:	**true**
Preview:	.._....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Purchase Order.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\Purchase Order.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@$.!.}}.&.VI.....Y.....gU..b.b..l..Bg....bh .$.....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\Purchase Order.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	42

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Entropy (8bit):	4.2704265780462904
Encrypted:	false
SSDEEP:	3:oNUWJRW1QK4q6:oNNJAaND
MD5:	618AC53B37F2EB68D08319403146536E
SHA1:	67C1E821D177E25C98B184DAF5EBDD3F4D6690EB
SHA-256:	CFFFF74893EDC2CF68D57EFC43C36EDB3B01F5AA38EA574EF0BBAA7EDFCD3348
SHA-512:	B6B200880B4F880D22EFED2AB2A5DF6FD9D437C74BC8A4D9C29002837684773A5885C55694718D759E42758D250F4A461FEAC26636A04AFE1A6B0F9DC67E080
Malicious:	false
Preview:	C:\Users\user\Desktop\Purchase Order.exe

C:\Users\user\AppData\Roaming\sWTAwlQUDpm.exe	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	493568
Entropy (8bit):	7.678704961445741
Encrypted:	false
SSDEEP:	12288:uBbYwVLa/V7PVGjWUUrhr4MTigNFxKAHszQ0lxZ:GbYGe7uWdhM8xxtszRd
MD5:	3F4E18FA2E1404E2C8F7F7E58C0DAE4E
SHA1:	435587D7A9213B7F42086D2B39D06C90E6D8391A
SHA-256:	5A608E9DAF5ACA1CCF0E6EF4CDBC826A02BA11037626787D6A35D2FF08CDB08A
SHA-512:	985E5F971B2D53E2FF0D4A327DB326D03BF45A83A003CF841B91B42F4BF98B3A38F8CF0E6B4204AF39FFCD3BB02FF659D58B27013B78AA425B02FF0EA6B4561E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zi.....P..r..... .....@.. ..... .@.....w...O.....8..... ....H.....text....q... ...r..... ..`.rsrc.....t.....@..@.reloc..... .....@..B.....H.....$.....H.....0.....(....(.....(.....o ....*.....(!.....("......(#.....($.....(%....*N..(....o....(&....*&.. ('....*.s(.....s).....s*.....s+.....s,.....*....0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*.0.....~....o1....+..*.0..<.....~.....(2.....,!r... p.....(3...o4...s5.....~.....+..*.0.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.678704961445741
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Purchase Order.exe
File size:	493568
MD5:	3f4e18fa2e1404e2c8f7f7e58c0dae4e
SHA1:	435587d7a9213b7f42086d2b39d06c90e6d8391a
SHA256:	5a608e9daf5aca1ccf0e6ef4cdbc826a02ba11037626787d6a35d2ff08cdb08a
SHA512:	985e5f971b2d53e2ff0d4a327db326d03bf45a83a003cf841b91b42f4bf98b3a38f8cf0e6b4204af39ffcd3bb02ff659d58b27013b78aa425b02ff0ea6b4561e
SSDEEP:	12288:uBbYwVLa/V7PVGjWUUrhr4MTigNFxKAHszQ0lxZ:GbYGe7uWdhM8xxtszRd
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zi.....P..r..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4791ca
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:	0x8E9F697A [Sat Oct 28 13:58:18 2045 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x771d0	0x77200	False	0.86247786595	data	7.69202666714	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7a000	0x1114	0x1200	False	0.381076388889	data	4.9255976369	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c000	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
11/23/21-07:44:17.237267	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52480	8.8.8.8	192.168.2.5
11/23/21-07:44:22.918501	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51165	8.8.8.8	192.168.2.5
11/23/21-07:44:28.415590	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	57587	8.8.8.8	192.168.2.5
11/23/21-07:44:39.605379	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	64936	8.8.8.8	192.168.2.5
11/23/21-07:44:50.649318	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54302	8.8.8.8	192.168.2.5
11/23/21-07:45:01.674443	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65307	8.8.8.8	192.168.2.5

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/23/21-07:45:29.342544	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	65447	8.8.8.8	192.168.2.5
11/23/21-07:45:46.116939	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	63183	8.8.8.8	192.168.2.5
11/23/21-07:45:51.703391	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	60151	8.8.8.8	192.168.2.5
11/23/21-07:46:03.029157	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	6272	192.168.2.5	194.5.97.210

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 23, 2021 07:44:17.215949059 CET	192.168.2.5	8.8.8.8	0x9fd2	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:22.896964073 CET	192.168.2.5	8.8.8.8	0xca47	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:28.394016981 CET	192.168.2.5	8.8.8.8	0x8d93	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:34.027271986 CET	192.168.2.5	8.8.8.8	0xd2b7	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:39.583848953 CET	192.168.2.5	8.8.8.8	0x4a4b	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:45.083228111 CET	192.168.2.5	8.8.8.8	0x2a33	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:50.627996922 CET	192.168.2.5	8.8.8.8	0xa113	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:56.151756048 CET	192.168.2.5	8.8.8.8	0x3363	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:01.652332067 CET	192.168.2.5	8.8.8.8	0xa54d	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:07.180596113 CET	192.168.2.5	8.8.8.8	0x4f38	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:12.773217916 CET	192.168.2.5	8.8.8.8	0x1683	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:18.275168896 CET	192.168.2.5	8.8.8.8	0x4378	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:23.829754114 CET	192.168.2.5	8.8.8.8	0xb037	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:29.321582079 CET	192.168.2.5	8.8.8.8	0xda8a	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:34.933257103 CET	192.168.2.5	8.8.8.8	0x9222	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:40.460719109 CET	192.168.2.5	8.8.8.8	0x943a	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:46.097528934 CET	192.168.2.5	8.8.8.8	0x1852	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:51.681828022 CET	192.168.2.5	8.8.8.8	0xf4b4	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:57.295866966 CET	192.168.2.5	8.8.8.8	0x23c5	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)
Nov 23, 2021 07:46:02.808727026 CET	192.168.2.5	8.8.8.8	0x336e	Standard query (0)	billie4.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

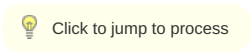
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2021 07:44:17.237267017 CET	8.8.8.8	192.168.2.5	0x9fd2	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:22.918500900 CET	8.8.8.8	192.168.2.5	0xca47	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2021 07:44:28.415590048 CET	8.8.8.8	192.168.2.5	0x8d93	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:34.048892975 CET	8.8.8.8	192.168.2.5	0xd2b7	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:39.605379105 CET	8.8.8.8	192.168.2.5	0x4a4b	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:45.100925922 CET	8.8.8.8	192.168.2.5	0x2a33	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:50.649317980 CET	8.8.8.8	192.168.2.5	0xa113	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:44:56.171714067 CET	8.8.8.8	192.168.2.5	0x3363	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:01.674443007 CET	8.8.8.8	192.168.2.5	0xa54d	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:07.198613882 CET	8.8.8.8	192.168.2.5	0x4f38	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:12.793133020 CET	8.8.8.8	192.168.2.5	0x1683	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:18.294912100 CET	8.8.8.8	192.168.2.5	0x4378	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:23.849181890 CET	8.8.8.8	192.168.2.5	0xb037	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:29.342544079 CET	8.8.8.8	192.168.2.5	0xda8a	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:34.953414917 CET	8.8.8.8	192.168.2.5	0x9222	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:40.480710030 CET	8.8.8.8	192.168.2.5	0x943a	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:46.116939068 CET	8.8.8.8	192.168.2.5	0x1852	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:51.703391075 CET	8.8.8.8	192.168.2.5	0xf4b4	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:45:57.315715075 CET	8.8.8.8	192.168.2.5	0x23c5	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)
Nov 23, 2021 07:46:02.829051018 CET	8.8.8.8	192.168.2.5	0x336e	No error (0)	billie4.ddns.net		194.5.97.210	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Purchase Order.exe PID: 4948 Parent PID: 5312

General

Start time:	07:44:02
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase Order.exe"
Imagebase:	0xa70000
File size:	493568 bytes
MD5 hash:	3F4E18FA2E1404E2C8F7F7E58C0DAE4E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.260337804.000000000312F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.261218037.00000000040E1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.261218037.00000000040E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.261218037.00000000040E1000.00000004.00000001.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: 2940 Parent PID: 4948

General

Start time:	07:44:09
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\sWTAwlQUDpm" /XML "C:\Users\user\AppData\Local\Temp\tmpFF67.tmp
Imagebase:	0x10c0000
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: 3848 Parent PID: 2940

General

Start time:	07:44:10
Start date:	23/11/2021
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: Purchase Order.exe PID: 2840 Parent PID: 4948

General

Start time:	07:44:10
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xcb0000
File size:	493568 bytes
MD5 hash:	3F4E18FA2E1404E2C8F7F7E58C0DAE4E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.514093712.0000000004451000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.510612941.0000000001400000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.510612941.0000000001400000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.516783135.0000000005C30000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.516783135.0000000005C30000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.513024868.0000000001730000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.513024868.0000000001730000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.509365335.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.509365335.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.509365335.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.514370660.0000000004632000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.514370660.0000000004632000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.256909060.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.256909060.0000000000402000.00000040.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 00000003.00000000.256909060.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.258283803.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.258283803.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.258283803.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.257814909.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.257814909.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.257814909.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.512869646.00000000016F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.512869646.00000000016F0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.512970824.0000000001720000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.512970824.0000000001720000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.517345477.0000000005FF0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.517345477.0000000005FF0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.517345477.0000000005FF0000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.513074700.0000000001770000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.513074700.0000000001770000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.510571872.00000000013E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.510571872.00000000013E0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.514554854.0000000004851000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.514554854.0000000004851000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.257324506.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.257324506.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.257324506.0000000000402000.00000040.00000001.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: 4664 Parent PID: 2840

General

Start time:	07:44:13
Start date:	23/11/2021
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\tmp5DEB.tmp
Imagebase:	0x10c0000
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: 5148 Parent PID: 4664

General

Start time:	07:44:15
Start date:	23/11/2021
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: Purchase Order.exe PID: 4576 Parent PID: 904

General

Start time:	07:44:16
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase Order.exe" 0
Imagebase:	0x3c0000
File size:	493568 bytes
MD5 hash:	3F4E18FA2E1404E2C8F7F7E58C0DAE4E
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: 00000007.00000002.293600942.0000000003B31000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.293600942.0000000003B31000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.293600942.0000000003B31000.00000004.00000001.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: 2960 Parent PID: 4576

General

Start time:	07:44:21
Start date:	23/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\sWTAwlQUDpm" /XML "C:\Users\user\AppData\Local\Temp\tmp2DF9.tmp
Imagebase:	0x10c0000
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: 4908 Parent PID: 2960

General

Start time:	07:44:22
Start date:	23/11/2021
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: Purchase Order.exe PID: 5872 Parent PID: 4576

General

Start time:	07:44:24
Start date:	23/11/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xe50000
File size:	493568 bytes
MD5 hash:	3F4E18FA2E1404E2C8F7F7E58C0DAE4E
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.00000000.290105146.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.290105146.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.290105146.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000002.304942297.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.304942297.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.304942297.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.288438984.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.288438984.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.288438984.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.288897596.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.288897596.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.288897596.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.305808689.0000000004611000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.305808689.0000000004611000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.305776301.0000000003611000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.305776301.0000000003611000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000E.00000000.289395103.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000000.289395103.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000000.289395103.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis