ID: 431795
Sample Name:
POInvoiceOrderIuVvcl0VWEOAmXy.exe
Cookbook: default.jbs
Time: 10:35:15
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Copyright Joe Security LLC 2021

Copyright Joe Security LLC 2021

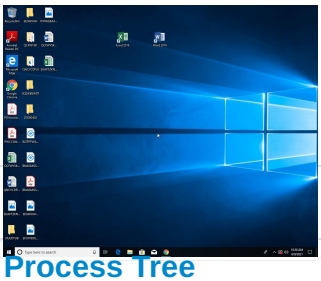
Analysis Report POInvoiceOrderIuVvcl0VWEOAmXy.exe

Overview

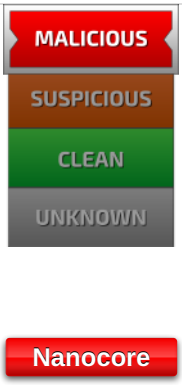
General Information

Sample Name:	POInvoiceOrderIuVvcl0VWEOAmXy.exe
Analysis ID:	431795
MD5:	fb1eb909e34c22f..
SHA1:	f301810874ac9b5.
SHA256:	acfd6ceddcb0f24…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



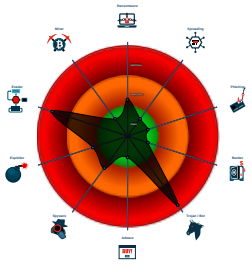
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- POInvoiceOrderIuVvcl0VWEOAmXy.exe (PID: 6140 cmdline: 'C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe' MD5: FB1EB909E34C22F21310565CF4B71563)
  - schtasks.exe (PID: 5904 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KbWjJvsRSE' /XML 'C:\Users\user\AppData\Local\Temp\tmp220B.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - POInvoiceOrderIuVvcl0VWEOAmXy.exe (PID: 1084 cmdline: C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe MD5: FB1EB909E34C22F21310565CF4B71563)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "1fb9e357-3073-471b-ab6f-630ca123",
  "Group": "kmt",
  "Domain1": "kkmmtt.duckdns.org",
  "Domain2": "kmttk.hopto.org",
  "Port": 6060,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.463995578.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000002.463995578.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.463995578.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000004.00000002.471906228.000000000570000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000004.00000002.471906228.000000000570000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost

Click to see the 20 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.POInvoiceOrderIuVvcl0VWEOAmXy.exe.5730000.8.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
4.2.POInvoiceOrderIuVvcl0VWEOAmXy.exe.5730000.8.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
4.2.POInvoiceOrderIuVvcl0VWEOAmXy.exe.4351990.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
4.2.POInvoiceOrderIuVvcl0VWEOAmXy.exe.4351990.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
4.2.POInvoiceOrderIuVvcl0VWEOAmXy.exe.4351990.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 46 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

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

Copyright Joe Security LLC 2021

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

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

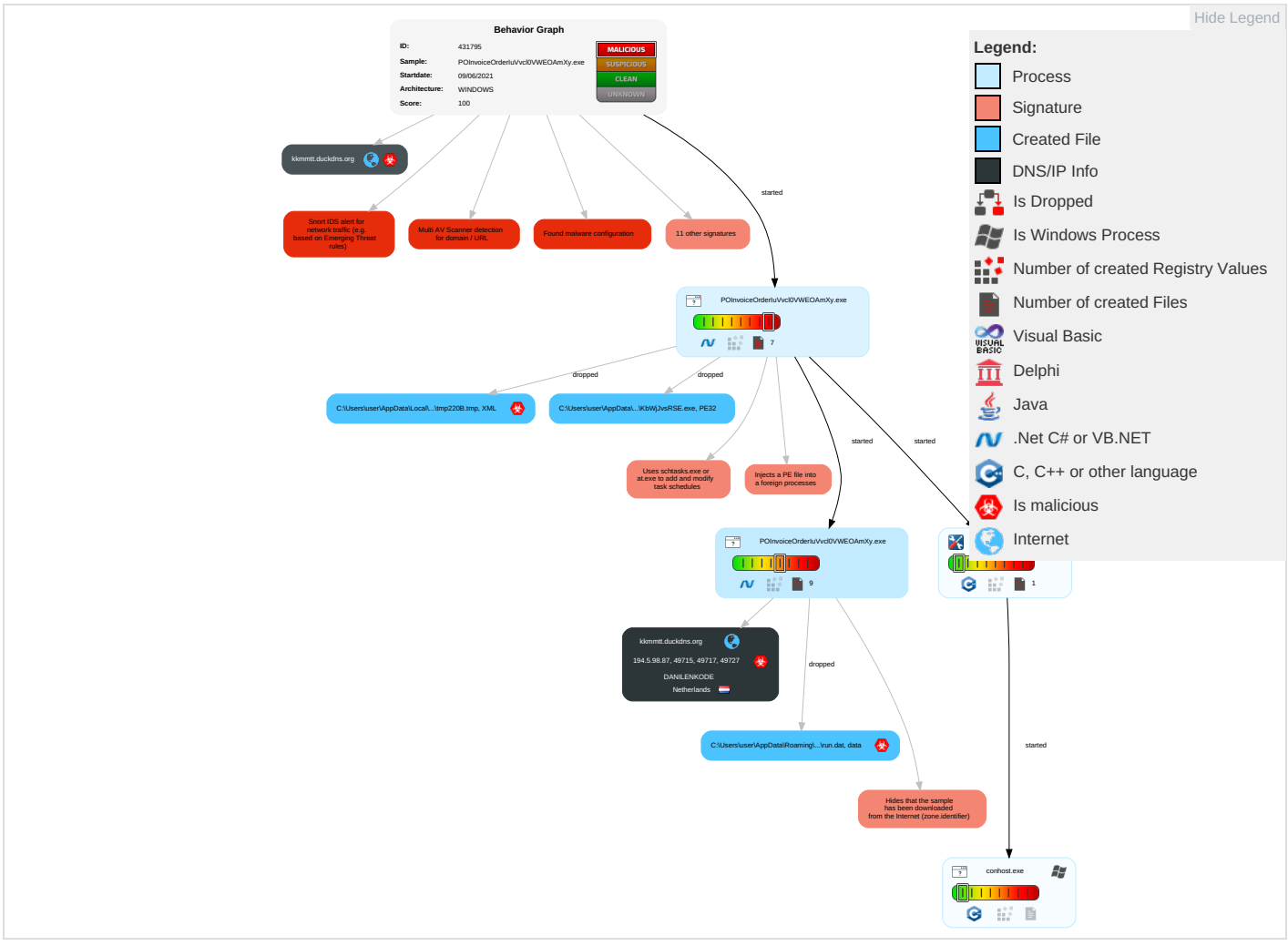
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Command and Scripting Interpreter 2	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	Encrypted Channel 1	Eave Insec Netw Com
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	Non-Standard Port 1	Explo Redi Calls
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explo Track Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 1 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Mani Devi Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Deni Servi

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

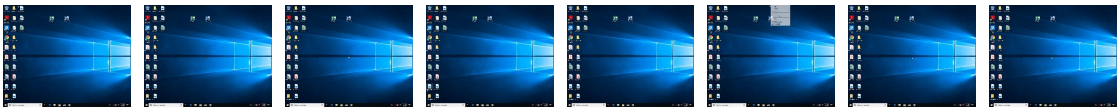
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.POInvoiceOrderIuVvcl0VWEOAmXy.exe.5c60000.11.unpack	100%	Avira	TR/NanoCore.fadte		Download File
4.0.POInvoiceOrderIuVvcl0VWEOAmXy.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.POInvoiceOrderIuVvcl0VWEOAmXy.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.POInvoiceOrderIuVvcl0VWEOAmXy.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
kkmmtt.duckdns.org	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.sajatypeworks.com5	0%	Avira URL Cloud	safe	
kmttk.hopto.org	7%	Virustotal		Browse
kmttk.hopto.org	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comn-u	0%	Avira URL Cloud	safe	
kkmmtt.duckdns.org	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	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.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0e	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fonts.comt	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cnl-p	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/r	0%	Avira URL Cloud	safe	
http://www.fontbureau.comionoO	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/O	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/O	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/O	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fontbureau.comion	0%	URL Reputation	safe	
http://www.fonts.comn4	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/=	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/=	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/=	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/z	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	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/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/s	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	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/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
http://www.sandoll.co.krnta	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/MI	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
kkmmtt.duckdns.org	194.5.98.87	true	true	• 1%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
kmttk.hopto.org	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
kkmmtt.duckdns.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.87	kkmmtt.duckdns.org	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431795

Copyright Joe Security LLC 2021

Start date:	09.06.2021
Start time:	10:35:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 23s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	POInvoiceOrderIuVvcl0VWEOAmXy.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/6@18/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.2%) • Quality average: 30.6% • Quality standard deviation: 37.8%
HCA Information:	• Successful, ratio: 82% • 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
10:36:08	API Interceptor	946x Sleep call for process: POInvoiceOrderIuVvcl0VWEOAmXy.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.87	Invoice_orderYscFwfO1peuGl0w.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	payment invoice.exe	Get hash	malicious	Browse	• 194.5.98.23
	#RFQ ORDER484475577797.exe	Get hash	malicious	Browse	• 194.5.98.120
	b6yzWugw8V.exe	Get hash	malicious	Browse	• 194.5.98.107

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0041#Receipt.pif.exe	Get hash	malicious	Browse	• 194.5.98.180
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.18
	SecuriteInfo.com.Trojan.PackedNET.820.24493.exe	Get hash	malicious	Browse	• 194.5.97.61
	DHL_file.exe	Get hash	malicious	Browse	• 194.5.98.145
	BBS FX.xlsx	Get hash	malicious	Browse	• 194.5.97.61
	GpnPv433gb.exe	Get hash	malicious	Browse	• 194.5.98.11
	Kj7tTd1Zimp0cil.exe	Get hash	malicious	Browse	• 194.5.97.197
	Resume.exe	Get hash	malicious	Browse	• 194.5.98.8
	SecuriteInfo.com.Trojan.DownLoader39.38629.28832.exe	Get hash	malicious	Browse	• 194.5.98.145
	SecuriteInfo.com.Variant.Razy.840898.18291.exe	Get hash	malicious	Browse	• 194.5.98.144
	8LtwhjD2Qm.exe	Get hash	malicious	Browse	• 194.5.98.107
	Receiptn.exe	Get hash	malicious	Browse	• 194.5.98.180
	soa5.exe	Get hash	malicious	Browse	• 194.5.98.48
	soa5.exe	Get hash	malicious	Browse	• 194.5.98.48
	68Aj4oxPok.exe	Get hash	malicious	Browse	• 194.5.98.144

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\POInvoiceOrderIuVvcl0VWEOAmXy.exe.log	
Process:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	false
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..

C:\Users\user\AppData\Local\Temp\tmp220B.tmp	
Process:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.195851646316711
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBn0tn:cbh47TlNQ//rydbz9I3YODOLNdq3Fy
MD5:	6BD2FC1377B3D6119F378DD2802ED9AB
SHA1:	E45F4CE47ED5253087DC3C91EDCDF6148BEF6624
SHA-256:	A055D15B0C016003FEEF850630AE264447E960B36E5AF3AF59795C31C9F0A688
SHA-512:	225AD55642A9D82BF502E08C424579F2F187639B69BDCFC34E16146B747166D83BBC6F2177502877962472BB0C1EC00B5AAFA6FE6954F961989B09EDB512B0FD
Malicious:	**true**
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp220B.tmp

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>.. </Pri
ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte
ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

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

Process:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
File Type:	data
Category:	dropped
Size (bytes):	2728
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	48:Ik/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH8Uk/t3FmH87:ft3Ucrt3Ucrt3Ucrt3Ucrt3Ucrt3UcrN
MD5:	3F16EC9869DEDFFEC07792CA71B87AB5
SHA1:	124F3AAEB04E11DEA7361736CE472750D237D3D2
SHA-256:	1A187F3EF38284FF4EE2B20D6021C884E42FC72284F2DA858D7E389CE9C7D0E9
SHA-512:	8DDE0277C2F8CF1CEF64B1EDF120C4A239619FBE9513C833C94B9A429984ECB8AD2A346FD9E333270207951021CCB0CA08FFCDF2ADE538AAFC2B5FAAA1ADF 0A2
Malicious:	false
Reputation:	low

Preview:

Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL....f.Z#.|...@HkG....G..O*V..........pz...."....r...w&&|..c..3}~.....~...os..f.......4..1
.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL....f.Z#.|...@HkG....G..O*V..........pz...."...
.r...w&&|..c..3}~.....~...os..f.......4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B.......].P...W.4C}uL....f.Z#.|...@H
kG....G..O*V..........pz...."....r...w&&|..c..3}~.....~...os..f.......4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.....@.3..{...grv+V...B...
....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V..........pz...."....r...w&&|..c..3}~.....~...os..f.......4..1.gJ.'.d".L...A.t...F.{....C.|&.wGj.h\.3.

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

Process:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:mctn:mcn
MD5:	D6F53F9D52EE3C43FAAB54C8BBDCDB9B
SHA1:	FC2E188E00AFF335ABF17FB3319433CEE7CBC77A
SHA-256:	93FB74B9C257EF909456FB14BDE732BE75C99B21F66C6CD31BD5AE51614F8B4E
SHA-512:	FB68328E003834C01595D46C036CF042F387662B6164942A8ABD5EEAA5797AB0D9C0E2AE5BDFA9E9C7B66C5186748EC728FEABB7C196E57F2EFD216FD3D2A5 4
Malicious:	**true**
Reputation:	low

Preview:

.@..m+.H

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

Process:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	919552
Entropy (8bit):	7.392987782971905
Encrypted:	false
SSDEEP:	24576:SRjfsacU2VITgLiflegZKnWV0trUGrO2:QmITtZgWurnZ
MD5:	FB1EB909E34C22F21310565CF4B71563
SHA1:	F301810874AC9B59AEF7C5CA3D8377E35E4906BA
SHA-256:	ACFD6CEDDCB0F24E6A170EB64CFBBB1AF4876BCDA5FB572C36330B1F6208A84E
SHA-512:	E4D3C5A58D21FCC3E7A3D3AEC066C0A7B9CCC83B3328813D9E13F16085B1BF5A5E7FA90D1145D5EE7D15D045F9FA66169C4448B79D761EC2B9A1C8C75E768 3
Malicious:	false
Reputation:	low

Preview:

MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L...~`.`..............P..P...........o... ....@.. ....`..........
..@..................................n..O..........................@.......m.. ....H............text....O... ...P................. ..`.rsrc...............R.............@..@.reloc
.......@......................@..B.................n......H...........T:...0............(....(..........(.....o ....*.....................(!......("......(#......($......(%....*N..(....oS...
(&....*&..('....*.s(........s)........s*........s+........s,........*....0...........~....o-....+..*.0...........~....o.....+..*.0...........~....o/....+..*.0...........~....o0....+..*.0...........~....o1....+..*..(2...*6..o3...
(4...*&...o5...*.0..............,...+...(6...s7.....*&..(2....*.

C:\Users\user\AppData\Roaming\KbWjJvsRSE.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.392987782971905
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:	POInvoiceOrderIuVvcl0VWEOAmXy.exe
File size:	919552
MD5:	fb1eb909e34c22f21310565cf4b71563
SHA1:	f301810874ac9b59aef7c5ca3d8377e35e4906ba
SHA256:	acfd6ceddcb0f24e6a170eb64cfbbb1af4876bcda5fb572c36330b1f6208a84e
SHA512:	e4d3c5a58d21fcc3e7a3d3aec066c0a7b9ccc83b3328813d9e13f16085b1bf5a5e7fa90d1145d5ee7d15d045f9fa66169c4448b79d761ec2b9a1c8c75e768073
SSDEEP:	24576:SRjfsacU2VITgLiflegZKnWV0trUGrO2:QmITtZgWurnZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...~``.....P..P.....o... .....@.. .....`.....@.....

File Icon

Icon Hash:	e4ccccc4d6c6ced0

Static PE Info

General

Entrypoint:	0x4c6f12
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:	0x60C0607E [Wed Jun 9 06:32:30 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727

General

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	0xc4f18	0xc5000	False	0.824205117782	data	7.64208263099	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc8000	0x1b3d4	0x1b400	False	0.163507024083	data	3.50216689317	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe4000	0xc	0x200	False	0.044921875	data	0.0980041756627	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
06/09/21-10:36:21.025415	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	6060	192.168.2.3	194.5.98.87
06/09/21-10:36:27.238432	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	6060	192.168.2.3	194.5.98.87
06/09/21-10:36:33.643583	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	6060	192.168.2.3	194.5.98.87
06/09/21-10:36:39.965819	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	6060	192.168.2.3	194.5.98.87
06/09/21-10:36:47.045107	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	6060	192.168.2.3	194.5.98.87
06/09/21-10:36:53.291694	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	6060	192.168.2.3	194.5.98.87
06/09/21-10:36:59.519297	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	6060	192.168.2.3	194.5.98.87
06/09/21-10:37:05.825337	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	6060	192.168.2.3	194.5.98.87
06/09/21-10:37:12.192676	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	6060	192.168.2.3	194.5.98.87
06/09/21-10:37:19.250964	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	6060	192.168.2.3	194.5.98.87
06/09/21-10:37:30.459866	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	6060	192.168.2.3	194.5.98.87
06/09/21-10:37:36.867895	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	6060	192.168.2.3	194.5.98.87
06/09/21-10:37:43.200507	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	6060	192.168.2.3	194.5.98.87
06/09/21-10:37:49.441608	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	6060	192.168.2.3	194.5.98.87
06/09/21-10:37:55.708033	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	6060	192.168.2.3	194.5.98.87
06/09/21-10:38:01.940654	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	6060	192.168.2.3	194.5.98.87

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-10:38:07.998819	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	6060	192.168.2.3	194.5.98.87

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 10:36:20.047811985 CEST	192.168.2.3	8.8.8.8	0xb33e	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:26.807152987 CEST	192.168.2.3	8.8.8.8	0x146d	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:33.197031021 CEST	192.168.2.3	8.8.8.8	0x5156	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:39.532572031 CEST	192.168.2.3	8.8.8.8	0x6289	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:46.335578918 CEST	192.168.2.3	8.8.8.8	0x64b2	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:52.856112957 CEST	192.168.2.3	8.8.8.8	0xcdf1	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:59.254034042 CEST	192.168.2.3	8.8.8.8	0xb180	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:05.541382074 CEST	192.168.2.3	8.8.8.8	0x944f	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:11.751173019 CEST	192.168.2.3	8.8.8.8	0xdf89	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:18.215631962 CEST	192.168.2.3	8.8.8.8	0xdc0f	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:25.377041101 CEST	192.168.2.3	8.8.8.8	0xdd4	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:30.022260904 CEST	192.168.2.3	8.8.8.8	0x35f2	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:36.421251059 CEST	192.168.2.3	8.8.8.8	0x97c0	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:42.762809992 CEST	192.168.2.3	8.8.8.8	0x231c	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:49.167521000 CEST	192.168.2.3	8.8.8.8	0x8da4	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:55.253063917 CEST	192.168.2.3	8.8.8.8	0x182f	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:38:01.676273108 CEST	192.168.2.3	8.8.8.8	0x48bc	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 10:38:07.727155924 CEST	192.168.2.3	8.8.8.8	0x458	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 10:36:20.264655113 CEST	8.8.8.8	192.168.2.3	0xb33e	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:27.016743898 CEST	8.8.8.8	192.168.2.3	0x146d	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:33.408946037 CEST	8.8.8.8	192.168.2.3	0x5156	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:39.741951942 CEST	8.8.8.8	192.168.2.3	0x6289	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:46.378822088 CEST	8.8.8.8	192.168.2.3	0x64b2	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)

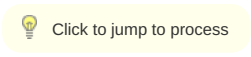
Copyright Joe Security LLC 2021

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 10:36:53.070564985 CEST	8.8.8.8	192.168.2.3	0xcdf1	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:36:59.297163963 CEST	8.8.8.8	192.168.2.3	0xb180	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:05.584774017 CEST	8.8.8.8	192.168.2.3	0x944f	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:11.966873884 CEST	8.8.8.8	192.168.2.3	0xdf89	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:18.426738977 CEST	8.8.8.8	192.168.2.3	0xdc0f	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:25.420192003 CEST	8.8.8.8	192.168.2.3	0xdd4	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:30.233668089 CEST	8.8.8.8	192.168.2.3	0x35f2	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:36.634321928 CEST	8.8.8.8	192.168.2.3	0x97c0	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:39.865470886 CEST	8.8.8.8	192.168.2.3	0x99ff	No error (0)	prda.aadg.msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)
Jun 9, 2021 10:37:42.976070881 CEST	8.8.8.8	192.168.2.3	0x231c	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:49.210297108 CEST	8.8.8.8	192.168.2.3	0x8da4	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:37:55.461719990 CEST	8.8.8.8	192.168.2.3	0x182f	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:38:01.719487906 CEST	8.8.8.8	192.168.2.3	0x48bc	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 10:38:07.770628929 CEST	8.8.8.8	192.168.2.3	0x458	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: POInvoiceOrderIuVvcl0VWEOAmXy.exe PID: 6140 Parent PID: 5584

General

Start time:	10:36:00
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
Wow64 process (32bit):	true

Copyright Joe Security LLC 2021

Commandline:	'C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe'
Imagebase:	0x830000
File size:	919552 bytes
MD5 hash:	FB1EB909E34C22F21310565CF4B71563
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: 00000001.00000002.234767836.0000000003EF1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.234767836.0000000003EF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.234767836.0000000003EF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.234244146.0000000002F17000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5904 Parent PID: 6140

General

Start time:	10:36:15
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\KbWjJvsRSE' /XML 'C:\Users\user\AppData\Local\Temp\tmp220B.tmp'
Imagebase:	0xf40000
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: 1832 Parent PID: 5904

General

Start time:	10:36:15
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: POInvoiceOrderIuVvcl0VWEOAmXy.exe PID: 1084 Parent PID: 6140

General

Start time:	10:36:16
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\POInvoiceOrderIuVvcl0VWEOAmXy.exe
Imagebase:	0xc60000
File size:	919552 bytes
MD5 hash:	FB1EB909E34C22F21310565CF4B71563
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: 00000004.00000002.463995578.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.463995578.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.463995578.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.471906228.0000000005730000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.471906228.0000000005730000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.232483645.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.232483645.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.232483645.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.472266831.0000000005C50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.472266831.0000000005C50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.471023992.000000000433F000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.231248149.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.231248149.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.231248149.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.472281390.0000000005C60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.472281390.0000000005C60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.472281390.0000000005C60000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021