JoeSandbox Cloud BASIC

ID: 431840
Sample Name:
InvoicePOzGlybgcIc1vHasG.exe
Cookbook: default.jbs
Time: 12:25:52
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

Table of Contents 2
Analysis Report InvoicePOzGlybgcIc1vHasG.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Signature Overview 6
AV Detection: 6
Networking: 6
E-Banking Fraud: 6
System Summary: 6
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 9
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 12
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 16
Data Directories 16
Sections 16
Resources 16
Imports 16
Version Infos 16
Network Behavior 16
Snort IDS Alerts 16
Network Port Distribution 17
TCP Packets 17
UDP Packets 17
DNS Queries 17
DNS Answers 17

Copyright Joe Security LLC 2021

Code Manipulations 18
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: InvoicePOzGlybgcIc1vHasG.exe PID: 2168 Parent PID: 5628 18
General 18
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Analysis Process: schtasks.exe PID: 5400 Parent PID: 2168 19
General 19
File Activities 19
File Read 19
Analysis Process: conhost.exe PID: 4812 Parent PID: 5400 19
General 19
Analysis Process: InvoicePOzGlybgcIc1vHasG.exe PID: 5588 Parent PID: 2168 20
General 20
Analysis Process: InvoicePOzGlybgcIc1vHasG.exe PID: 6056 Parent PID: 2168 20
General 20
File Activities 21
File Created 21
File Deleted 21
File Written 21
File Read 21
Disassembly 21
Code Analysis 21

Copyright Joe Security LLC 2021

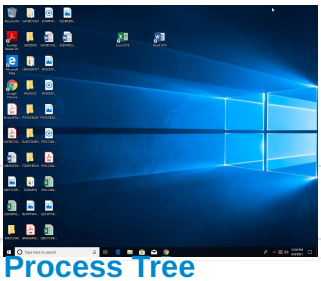
Analysis Report InvoicePOzGlybgcIc1vHasG.exe

Overview

General Information

Sample Name:	InvoicePOzGlybgcIc1vHasG.exe
Analysis ID:	431840
MD5:	372a0f073e924d0.
SHA1:	4d7784beff50b79..
SHA256:	babc65e527c875..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

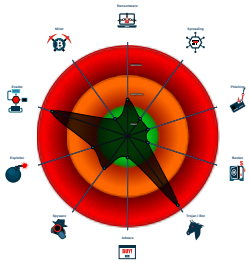
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- 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…

Classification



Process Tree

- **System is w10x64**
- InvoicePOzGlybgcIc1vHasG.exe (PID: 2168 cmdline: 'C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe' MD5: 372A0F073E924D0411A1FB660840A4CB)
  - schtasks.exe (PID: 5400 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OWNYQkAV' /XML 'C:\Users\user\AppData\Local\Temp\tmp6CCF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - InvoicePOzGlybgcIc1vHasG.exe (PID: 5588 cmdline: C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe MD5: 372A0F073E924D0411A1FB660840A4CB)
  - InvoicePOzGlybgcIc1vHasG.exe (PID: 6056 cmdline: C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe MD5: 372A0F073E924D0411A1FB660840A4CB)
- **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
00000004.00000000.241321715.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000000.241321715.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000000.241321715.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000000.00000002.247872551.0000000002D97000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.479356402.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 15 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.InvoicePOzGlybgcIc1vHasG.exe.4a2d893.13.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
4.2.InvoicePOzGlybgcIc1vHasG.exe.4a2d893.13.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
4.2.InvoicePOzGlybgcIc1vHasG.exe.367a59c.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
4.2.InvoicePOzGlybgcIc1vHasG.exe.367a59c.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
0.2.InvoicePOzGlybgcIc1vHasG.exe.3ea8e00.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 61 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

Multi AV Scanner detection for dropped file

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

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

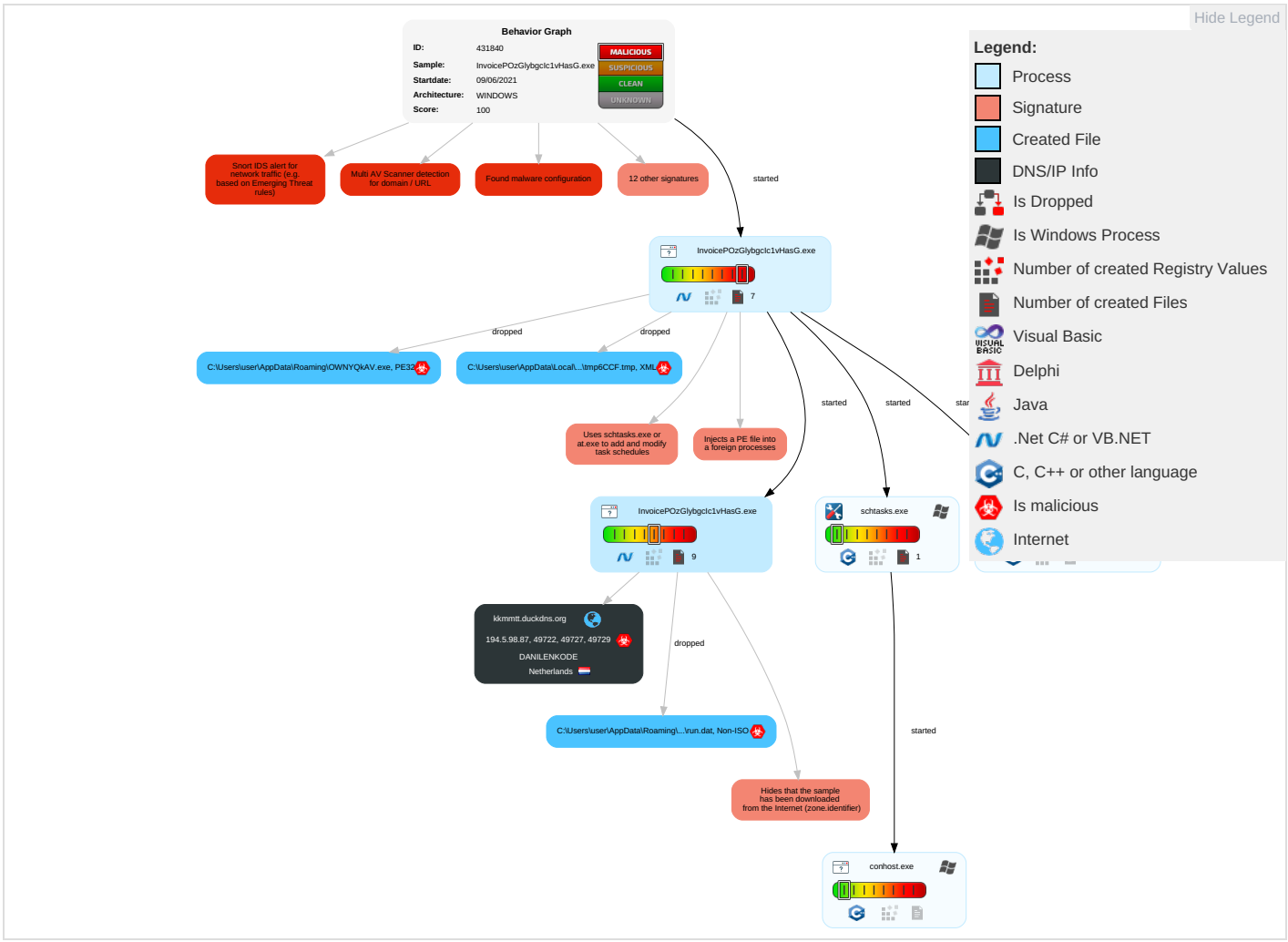
Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effect
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	Ingress Tool Transfer 1	Eaves Insecu Netwo Comm
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploi Redire Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 3	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Remote Access Software 1	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Application Layer Protocol 1	Manip Devic Comm
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	Application Layer Protocol 2 1	Jamm Denia Servic

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
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	Rogue Acces
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	Down Insecu Protoc
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	Rogue Base

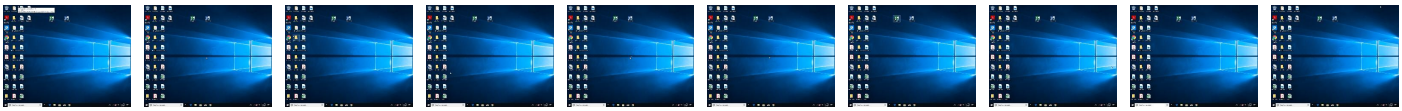
Behavior Graph



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

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\OWNYQkAV.exe	11%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.0.InvoicePOzGlybgcIc1vHasG.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.0.InvoicePOzGlybgcIc1vHasG.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.InvoicePOzGlybgcIc1vHasG.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.tiro.com)(u	0%	Avira URL Cloud	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.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/a-e	0%	Avira URL Cloud	safe	
kmttk.hopto.org	7%	Virustotal		Browse
kmttk.hopto.org	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.tiro.comnm	0%	Avira URL Cloud	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/ana	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ana	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	0%	URL Reputation	safe	
http://www.fonts.comn	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.founder.com.cn/cn/i	0%	Avira URL Cloud	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.sandoll.co.krH	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.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y	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/V	0%	URL Reputation	safe	
http://en.wWD	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.coms	0%	Avira URL Cloud	safe	
http://www.founder.com.c	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.founder.com.c	0%	URL Reputation	safe	
http://www.founder.com.c	0%	URL Reputation	safe	
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/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	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.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.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.fonts.comnn(6	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	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.sajatypeworks.coma-d	0%	URL Reputation	safe	
http://www.sajatypeworks.coma-d	0%	URL Reputation	safe	
http://www.sajatypeworks.coma-d	0%	URL Reputation	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:	431840
Start date:	09.06.2021
Start time:	12:25:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	InvoicePOzGlybgcIc1vHasG.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@8/6@17/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.7% (good quality ratio 2.6%) • Quality average: 53.5% • Quality standard deviation: 21.1%
HCA Information:	• Successful, ratio: 92% • 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
12:26:51	API Interceptor	958x Sleep call for process: InvoicePOzGlybgcIc1vHasG.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.87	POInvoiceOrderIuVvcl0VWEOAmXy.exe	Get hash	malicious	Browse	
	Invoice_orderYscFwfO1peuGl0w.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
kkmmtt.duckdns.org	POInvoiceOrderIuVvcl0VWEOAmXy.exe	Get hash	malicious	Browse	• 194.5.98.87

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	POInvoiceOrderIuVvcl0VWEOAmXy.exe	Get hash	malicious	Browse	• 194.5.98.87
	payment invoice.exe	Get hash	malicious	Browse	• 194.5.98.23
	#RFQ ORDER484475577797.exe	Get hash	malicious	Browse	• 194.5.98.120
	b6yzWugw8V.exe	Get hash	malicious	Browse	• 194.5.98.107
	0041#Receipt.pif.exe	Get hash	malicious	Browse	• 194.5.98.180
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	j07ghiByDq.exe	Get hash	malicious	Browse	• 194.5.97.146
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.18
	SecuriteInfo.com.Trojan.PackedNET.820.24493.exe	Get hash	malicious	Browse	• 194.5.97.61
	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
	Kj7tTd1Zimp0ciI.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

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\InvoicePOzGlybgcIc1vHasG.exe.log	
Process:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.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#\3577 4dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp6CCF.tmp	
Process:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1641
Entropy (8bit):	5.198638736339874
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB9Ntn:cbh47TlNQ//rydbz9I3YODOLNdq3H
MD5:	65B8E874E8C7B722282D9EAE22636205
SHA1:	3911D252BE06E717C92BCB33596F612990551227
SHA-256:	EACBBD33FFFD20262DB15EB1844EDA88C36B74111D4E9AEE14F5AC6D9571D8B8

C:\Users\user\AppData\Local\Temp\tmp6CCF.tmp	
SHA-512:	6DD349238F0A147B64D91D541710524F7A9E8D005721EB4773845CF0FA9A84774CC76B089CC9E0D29D005D62737C76C282530C61BE5A4958AA3A117E66A1CF20
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.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\InvoicePOzGlybgcIc1vHasG.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:D8:o
MD5:	175E573A6A264D22DEF1E0549EE24B19
SHA1:	D304CB912B1E7CB1B3A38E4F6A06C073D2CD868D
SHA-256:	08D59D3DF6BB432EB397E6FDC2900B8180BB9F6877D7A9875526ABE2EC9E2F3C
SHA-512:	E6F6C2498C0444946B4954134FDFB339B83FA47B13A964C1BD0AEABE44F1FEC579F3D22FFA0CD4BC3557AD4727EDE1D7F7AC25288F1AC8459ECDC958892A29 5
Malicious:	**true**
Reputation:	low
Preview:	H,w.|+.H

C:\Users\user\AppData\Roaming\OWNYQkAV.exe	
Process:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	907264
Entropy (8bit):	7.374036796875479
Encrypted:	false
SSDEEP:	12288:LSZ+XIMV40XINxqkNgCrmpa5aFW5JV9JINdEW0YjrzzyKVfUhweevXTxh:LSZ+XUuqGmpjF8JV9JINSUjrzjUueeP
MD5:	372A0F073E924D0411A1FB660840A4CB
SHA1:	4D7784BEFF50B79D456D7D18EEDDF8FBAF66AFB9
SHA-256:	BABC65E527C875DBDD52604EF5FF4D2549958AAA59807A513D9008734754198C
SHA-512:	71E4AC3E3C3B3AFD92B78F4F0C1892EC12A33AFB149A5C5B096CBEBE5574F377442746AC641B9EA9B191A329DE170E657AF4BD19736E6AB7EE5B9B717D20A1 A0
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 11%
Reputation:	low

C:\Users\user\AppData\Roaming\OWNYQkAV.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...>..`..... .....N>... ...@....@.. ..... ..... ..@.....=..O....@..... ..... ..H.....text...T.... ... ..... ..`.rsrc.....@....."..... @..@.reloc .....@..B.....0>.....H.....0....J.....pQ.....*....("....(#.....($.....(%.....(&....*N..(....o....('....*&..((....*.s).....s*.....s+.....s,.. .....s-.....*Z.....o@.....*&..(A....*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}..... {....+.*...{.....,.+.....,.rq..psF...z..|....(...+*...{.....,.+..

C:\Users\user\AppData\Roaming\OWNYQkAV.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.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):	7.374036796875479
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	InvoicePOzGlybgcIc1vHasG.exe
File size:	907264
MD5:	372a0f073e924d0411a1fb660840a4cb
SHA1:	4d7784beff50b79d456d7d18eeddf8fbaf66afb9
SHA256:	babc65e527c875dbdd52604ef5ff4d2549958aaa59807a513d9008734754198c
SHA512:	71e4ac3e3c3b3afd92b78f4f0c1892ec12a33afb149a5c5b096cbebe5574f377442746ac641b9ea9b191a329de170e657af4bd19736e6ab7ee5b9b717d20a1a0
SSDEEP:	12288:LSZ+XlMV40XINxqkNgCrmpa5aFW5JV9JINdEW0YjrzzyKVfUhweevXTxh:LSZ+XUuqGmpjF8JV9JINSUjrzjUueeP
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...>..`..... .....N>... ...@....@.. ....@.....

File Icon

Icon Hash:	e4ccccc4d6c6ced0

Static PE Info

General

Entrypoint:	0x4c3e4e
Entrypoint Section:	.text

General

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:	0x60C08B3E [Wed Jun 9 09:34:54 2021 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	0xc1e54	0xc2000	False	0.819717249919	data	7.62703305973	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xc4000	0x1b3c8	0x1b400	False	0.163390553326	data	3.49742133558	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xe0000	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
06/09/21-12:27:05.347540	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49722	6060	192.168.2.3	194.5.98.87
06/09/21-12:27:11.955274	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	6060	192.168.2.3	194.5.98.87
06/09/21-12:27:18.591909	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	6060	192.168.2.3	194.5.98.87
06/09/21-12:27:26.227769	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	6060	192.168.2.3	194.5.98.87
06/09/21-12:27:32.508491	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	6060	192.168.2.3	194.5.98.87
06/09/21-12:27:38.991952	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	6060	192.168.2.3	194.5.98.87
06/09/21-12:27:45.373698	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	6060	192.168.2.3	194.5.98.87
06/09/21-12:27:51.829018	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	6060	192.168.2.3	194.5.98.87
06/09/21-12:27:58.228453	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	6060	192.168.2.3	194.5.98.87
06/09/21-12:28:04.638960	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	6060	192.168.2.3	194.5.98.87
06/09/21-12:28:11.071658	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	6060	192.168.2.3	194.5.98.87

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-12:28:17.698343	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	6060	192.168.2.3	194.5.98.87
06/09/21-12:28:24.292595	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	6060	192.168.2.3	194.5.98.87
06/09/21-12:28:30.871638	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	6060	192.168.2.3	194.5.98.87
06/09/21-12:28:37.316002	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	6060	192.168.2.3	194.5.98.87
06/09/21-12:28:45.059671	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	6060	192.168.2.3	194.5.98.87
06/09/21-12:28:51.529358	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	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 12:27:04.287075996 CEST	192.168.2.3	8.8.8.8	0xd595	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:11.482922077 CEST	192.168.2.3	8.8.8.8	0xb573	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:18.094793081 CEST	192.168.2.3	8.8.8.8	0x1f2b	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:25.791501999 CEST	192.168.2.3	8.8.8.8	0xccc4	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:32.241118908 CEST	192.168.2.3	8.8.8.8	0xc481	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:38.528435946 CEST	192.168.2.3	8.8.8.8	0x49c6	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:45.105695009 CEST	192.168.2.3	8.8.8.8	0xdb89	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:51.494065046 CEST	192.168.2.3	8.8.8.8	0xbc84	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:57.957446098 CEST	192.168.2.3	8.8.8.8	0xe658	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:04.355906010 CEST	192.168.2.3	8.8.8.8	0xa1e8	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:10.802517891 CEST	192.168.2.3	8.8.8.8	0x2e9d	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:17.245949030 CEST	192.168.2.3	8.8.8.8	0x40ad	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:23.821482897 CEST	192.168.2.3	8.8.8.8	0x55ab	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:30.405299902 CEST	192.168.2.3	8.8.8.8	0x5dcd	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:36.913624048 CEST	192.168.2.3	8.8.8.8	0x18d6	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:44.615665913 CEST	192.168.2.3	8.8.8.8	0x704e	Standard query (0)	kkmmtt.duckdns.org	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:51.258869886 CEST	192.168.2.3	8.8.8.8	0xa772	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 12:27:04.500524044 CEST	8.8.8.8	192.168.2.3	0xd595	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:11.692248106 CEST	8.8.8.8	192.168.2.3	0xb573	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 12:27:18.325519085 CEST	8.8.8.8	192.168.2.3	0x1f2b	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:26.002885103 CEST	8.8.8.8	192.168.2.3	0xccc4	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:32.283983946 CEST	8.8.8.8	192.168.2.3	0xc481	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:38.743886948 CEST	8.8.8.8	192.168.2.3	0x49c6	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:45.149060965 CEST	8.8.8.8	192.168.2.3	0xdb89	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:51.538211107 CEST	8.8.8.8	192.168.2.3	0xbc84	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:27:58.000147104 CEST	8.8.8.8	192.168.2.3	0xe658	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:04.398801088 CEST	8.8.8.8	192.168.2.3	0xa1e8	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:10.845539093 CEST	8.8.8.8	192.168.2.3	0x2e9d	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:17.457616091 CEST	8.8.8.8	192.168.2.3	0x40ad	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:24.045945883 CEST	8.8.8.8	192.168.2.3	0x55ab	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:30.647680044 CEST	8.8.8.8	192.168.2.3	0x5dcd	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:36.956681967 CEST	8.8.8.8	192.168.2.3	0x18d6	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:44.824454069 CEST	8.8.8.8	192.168.2.3	0x704e	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)
Jun 9, 2021 12:28:51.304605007 CEST	8.8.8.8	192.168.2.3	0xa772	No error (0)	kkmmtt.duckdns.org		194.5.98.87	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: InvoicePOzGlybgclc1vHasG.exe PID: 2168 Parent PID: 5628

General

Start time:	12:26:46
Start date:	09/06/2021

Path:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe'
Imagebase:	0x6c0000
File size:	907264 bytes
MD5 hash:	372A0F073E924D0411A1FB660840A4CB
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: 00000000.00000002.247872551.0000000002D97000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.248195118.0000000003D71000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.248195118.0000000003D71000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.248195118.0000000003D71000.00000004.00000001.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: 5400 Parent PID: 2168

General

Start time:	12:26:58
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OWNYQkAV' /XML 'C:\Users\user\AppData\Local\Temp\tmp6CCF.tmp'
Imagebase:	0x3d0000
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: 4812 Parent PID: 5400

General

Start time:	12:26:58
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: InvoicePOzGlybgcIc1vHasG.exe PID: 5588 Parent PID: 2168

General

Start time:	12:26:59
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe
Imagebase:	0x350000
File size:	907264 bytes
MD5 hash:	372A0F073E924D0411A1FB660840A4CB
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: InvoicePOzGlybgcIc1vHasG.exe PID: 6056 Parent PID: 2168

General

Start time:	12:27:00
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\InvoicePOzGlybgcIc1vHasG.exe
Imagebase:	0xdb0000
File size:	907264 bytes
MD5 hash:	372A0F073E924D0411A1FB660840A4CB
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: 00000004.00000000.241321715.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.241321715.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.241321715.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.479356402.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.479356402.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.479356402.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.240960733.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.240960733.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.240960733.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.485726963.0000000003649000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.486935224.0000000004647000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.486935224.0000000004647000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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