ID: 431785
Sample Name: payment invoice.exe
Cookbook: default.jbs
Time: 10:15:49
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

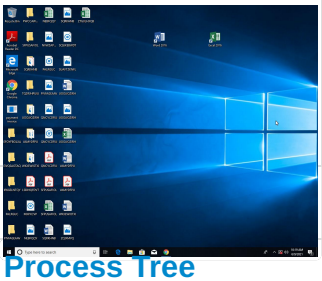
Analysis Report payment invoice.exe

Overview

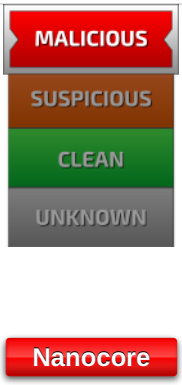
General Information

Sample Name:	payment invoice.exe
Analysis ID:	431785
MD5:	845d5dc8393bf76.
SHA1:	f83096a377039cf..
SHA256:	3aa4556bd929b5..
Tags:	exe NanoCore
Infos:	

Most interesting Screenshot:



Detection



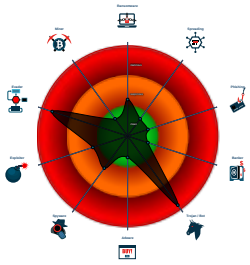
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- 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**
- payment invoice.exe (PID: 6660 cmdline: 'C:\Users\user\Desktop\payment invoice.exe' MD5: 845D5DC8393BF7652F744E7FA7DFB3C3)
  - schtasks.exe (PID: 6332 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GotewYBrdNy' /XML 'C:\Users\user\AppData\Local\Temp\tmpC705.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6320 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - payment invoice.exe (PID: 6568 cmdline: {path} MD5: 845D5DC8393BF7652F744E7FA7DFB3C3)
    - schtasks.exe (PID: 408 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD79F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4648 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- payment invoice.exe (PID: 976 cmdline: 'C:\Users\user\Desktop\payment invoice.exe' 0 MD5: 845D5DC8393BF7652F744E7FA7DFB3C3)
  - schtasks.exe (PID: 1688 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GotewYBrdNy' /XML 'C:\Users\user\AppData\Local\Temp\tmp70E1.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6236 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - payment invoice.exe (PID: 6504 cmdline: {path} MD5: 845D5DC8393BF7652F744E7FA7DFB3C3)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "64d6914b-2a13-4387-9ead-01228df9",
  "Group": "Default",
  "Domain1": "ifybest85fff.ddns.net",
  "Domain2": "194.5.98.23",
  "Port": 7600,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000000.464661919.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000B.00000000.464661919.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000000.464661919.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
0000000B.00000002.646691613.0000000003AB7000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000B.00000002.643057638.0000000002A61000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 78 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.payment invoice.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
11.2.payment invoice.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
11.2.payment invoice.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
11.2.payment invoice.exe.400000.0.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
11.2.payment invoice.exe.6f10000.23.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x16e3:$x1: NanoCore.ClientPluginHost • 0x171c:$x2: IClientNetworkHost
Click to see the 155 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

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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:

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:

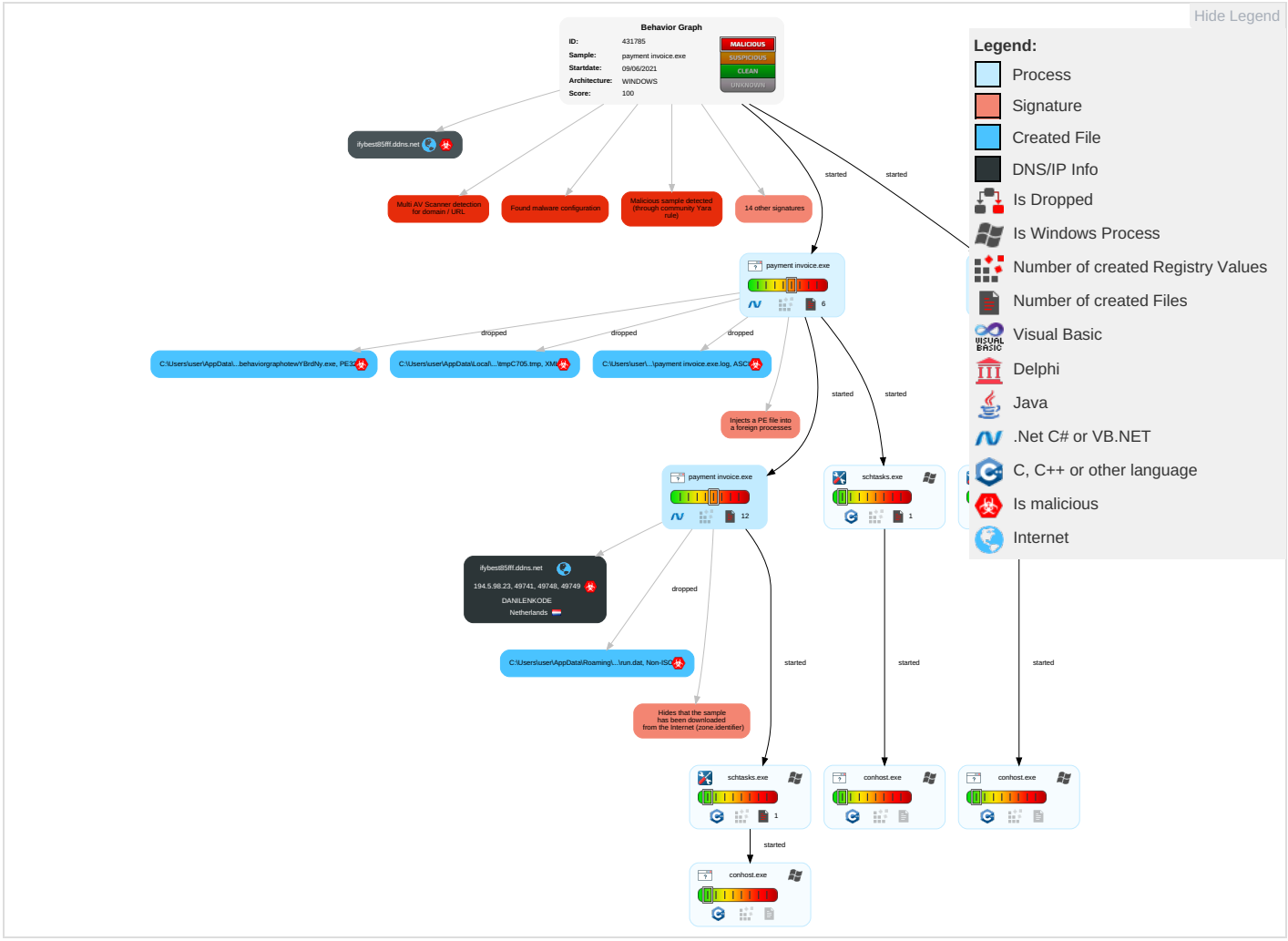
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1 1	Security Software Discovery 2 2 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

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
payment invoice.exe	45%	Virustotal		Browse
payment invoice.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
payment invoice.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\GotewYBrdNy.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\GotewYBrdNy.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.0.payment invoice.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.payment invoice.exe.3ac95f8.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
25.0.payment invoice.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.payment invoice.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
25.2.payment invoice.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.0.payment invoice.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
25.0.payment invoice.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
11.2.payment invoice.exe.5470000.17.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
ifybest85fff.ddns.net	7%	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.fontbureau.comic	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.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.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comahY	0%	Avira URL Cloud	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.carterandcone.coml	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.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.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.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://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://fontfabrik.com	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.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/	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.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	

Source	Detection	Scanner	Label	Link
http://www.sandoll.co.kr	0%	URL Reputation	safe	
ifybest85fff.ddns.net	7%	Virustotal		Browse
ifybest85fff.ddns.net	0%	Avira URL Cloud	safe	
194.5.98.23	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
ifybest85fff.ddns.net	194.5.98.23	true	true	• 7%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
ifybest85fff.ddns.net	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
194.5.98.23	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.23	ifybest85fff.ddns.net	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431785
Start date:	09.06.2021
Start time:	10:15:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 58s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	payment invoice.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:	27
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@15/11@12/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.8% (good quality ratio 0.5%) • Quality average: 44.6% • Quality standard deviation: 37.2%
HCA Information:	• Successful, ratio: 94% • 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
10:17:51	API Interceptor	668x Sleep call for process: payment invoice.exe modified
10:17:52	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\payment invoice.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.5.98.23	Asif Professional CV.exe	Get hash	malicious	Browse	
	Mwasiti Mnindy.exe	Get hash	malicious	Browse	
	Mwasiti Mnindy.exe	Get hash	malicious	Browse	
	INVs(2341).exe	Get hash	malicious	Browse	
	Bank Payment Copy.exe	Get hash	malicious	Browse	
	SWIFT COPY.exe	Get hash	malicious	Browse	
	payment invoice.exe	Get hash	malicious	Browse	
	Bank Payment Copy.exe	Get hash	malicious	Browse	
	ORDER SHEET - SUMMER 2021.exe	Get hash	malicious	Browse	
	Specifications Drawing Sketch Details-img.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ifybest85fff.ddns.net	Asif Professional CV.exe	Get hash	malicious	Browse	• 194.5.98.23

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DANILENKODE	#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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Ysur2E8xPs.exe	Get hash	malicious	Browse	• 194.5.97.61

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\payment invoice.exe.log	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp70E1.tmp	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.1594656034148185
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3NkOtn:cbha7JlNQV/rydbz9I3YODOLNdq3wo
MD5:	237C2B764584CA136806AD1FBE17F761
SHA1:	FE783B97447CF226C6FAA7F5AE7D972C2268A279
SHA-256:	9496A59C37BA72FC44EE6217E7D289A1D022BC8ECDE5197E5B5185D8051F79B3
SHA-512:	422B5D17D498781201CC0ADC36C3E0267900308DB09FF25D6B89E427D3ABBB52DB97A4A640BB7D68AEDF2014391D3FA12E2644D558952DABB51C77C09A383BA A
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp70E1.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>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpC705.tmp	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1656
Entropy (8bit):	5.1594656034148185
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3NkOtn:cbha7JlNQV/rydbz9I3YODOLNdq3wo
MD5:	237C2B764584CA136806AD1FBE17F761
SHA1:	FE783B97447CF226C6FAA7F5AE7D972C2268A279
SHA-256:	9496A59C37BA72FC44EE6217E7D289A1D022BC8ECDE5197E5B5185D8051F79B3
SHA-512:	422B5D17D498781201CC0ADC36C3E0267900308DB09FF25D6B89E427D3ABBB52DB97A4A640BB7D68AEDF2014391D3FA12E2644D558952DABB51C77C09A383BA
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>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmpD79F.tmp	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.082134358682254
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0V/nxtn:cbk4oL600QydbQxIYODOLedq38nj
MD5:	2718925F05BD1061363FC1DB90858234
SHA1:	0AB5DAFCED20DD659BF032004131A51397CD0886
SHA-256:	606E95C64E26A82B23885ABD2C0A3619DB9BE593FBFFF8345FE47E09273CEB06
SHA-512:	E95F45D6C3A24900856159ED3C59089766B1BC5E03AE226A272D725FB6D1FC69374074F5D4C94AB272A0C01CD121AA23FF096FF3CA281E14B3FA2D6BD290EE6
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCe
MD5:	0D6805D12813A857D50D42D6EE2CCAB0
SHA1:	78D83F009D842F21FE2AB0EAFFD00E5AAD1776F4
SHA-256:	182E0F8AA959549D61C66D049645BA8445D86AEAD2B8C3552A9836FA1E5BD484
SHA-512:	5B29496F3AB3CCB915CF37042F4956BB00E577B5F15457A5A739BE1BD50C481FB7E3297EED575DCA7A7BD30ECBC140DD3666CD7DEDD25DFB7AEB41A1B5BEI A4A
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E..... {...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators, with overstriking
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:MPh:MJ
MD5:	D00FDE39F5DC7B4ABDA8A17EFE02ED47
SHA1:	9314E390AED8DAF63A8F3507AA7F8D42959A4032
SHA-256:	1A9FD6E8ECD5DB86FA9AAF2350A49592499D2C25CD0C770817FD87DB365E68B5
SHA-512:	DEE193CCDEDA2CA8EABD12B8DEEB46FD5F261B7F46949FA34177E4EFF76CF5B133822B428AFDDBA296DEA1F4D37CB7AF20B09326F3FD138D5C821E9BAA85E71E
Malicious:	**true**
Preview:	2...j+.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYk:RzWDI3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDIvYVsRLY6oRDT6P2bfVn1:RzWDIfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A6
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,...]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	45
Entropy (8bit):	4.113206429278392
Encrypted:	false
SSDEEP:	3:oNN2+WVEcIqvdA:oNN2RucddA
MD5:	4E8183AE084261C1AF222E0DCC1BE281
SHA1:	8C8751A7FC261FDF903E0F1E47A7E9463855E12A
SHA-256:	EAC634E1CBF5C9F39FA4450A987DC15936083172CF8937C6DB6870D45C103A67
SHA-512:	76F424D13A6FC3CEB9A5ABFAE3F774C4D300D2E1321F6310E5DC363E0BF5C3BD8E4AEB086691DA393798993C026119C125F96435BBA86A71B88C67966CB717F
Malicious:	false
Preview:	C:\Users\user\Desktop\payment invoice.exe

C:\Users\user\AppData\Roaming\GotewYBrdNy.exe	
Process:	C:\Users\user\Desktop\payment invoice.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1043456
Entropy (8bit):	7.296264460943387
Encrypted:	false
SSDEEP:	12288:c1mk+vR1Hup6Z7Q/pDTXWILsbGRzcmtCN1/LFk6Hq0cpeTHKMgAbCZBvqpjExD07:Ox+vDOQZSz5UQRi
MD5:	845D5DC8393BF7652F744E7FA7DFB3C3
SHA1:	F83096A377039CFDBCFB930A98FD1B78691C4456
SHA-256:	3AA4556BD929B55C5A51EA8CD76865FD4E27B880EC483AA8A94582071CDEF24D
SHA-512:	E40303DC536090DA7B282A9A940765437C07ED3D497B0F81CDB92B9ABFC378D5EC54D96E946B69E368432B4FDE891A40681239056E3FC74FEA4568E4959D249
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...._!.`.....0.....n.... ... ....@.. .....`..... ..@.....S.... .....@..... ....H.....text...t.... ....`.rsrc..... .....@..@.rel oc.....@.....@..B.....P.....H.....X.....c.....s.....0.....*....0..".....r...p}.....}.....(.....(.....*...0.....{....(....r[..p(....:.... .0t. ....a%....^E.....M...a..... .....u.....8.....(..... /)..Z 1../a+....m...%.r]..p.%..{....(.....%.r...p.%..{....(.....%.r...p.%..{....(.....%.r...p.%..{....(... ..%..r...p.(.....(..... v`.UZ .^n.a8....r...p(....&.. aL..Z ..p.a8.....(....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.296264460943387
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:	payment invoice.exe
File size:	1043456
MD5:	845d5dc8393bf7652f744e7fa7dfb3c3
SHA1:	f83096a377039cfdbcfb930a98fd1b78691c4456

General

SHA256:	3aa4556bd929b55c5a51ea8cd76865fd4e27b880ec483aa8a94582071cdef24d
SHA512:	e40303dc536090da7b282a9a940765437c07ed3d497b0f81cdb92b9abfc378d5ec54d96e946b69e368432b4fde891a40681239056e3fc74fea4568e4959d249c
SSDEEP:	12288:c1mk+vR1Hup6Z7Q/pDTXWILsbGRzcmtCN1/LFk6Hq0cpeTHKMgAbCZBvqpjExD07:Ox+vDOQZSz5UQRi
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..._!.`.....0.....n.... ... ....@.. .....`.....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50016e
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:	0x60C0215F [Wed Jun 9 02:03:11 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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	0xfe174	0xfe200	False	0.613228410908	data	7.30117922021	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x102000	0x5e0	0x600	False	0.430338541667	data	4.17543821636	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x104000	0xc	0x200	False	0.044921875	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 10:17:53.225133896 CEST	192.168.2.6	8.8.8.8	0x288e	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:00.217374086 CEST	192.168.2.6	8.8.8.8	0xcc42	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:07.291168928 CEST	192.168.2.6	8.8.8.8	0x7ae	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:14.232737064 CEST	192.168.2.6	8.8.8.8	0x4293	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:21.288279057 CEST	192.168.2.6	8.8.8.8	0x1198	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:28.492014885 CEST	192.168.2.6	8.8.8.8	0x5b7e	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:35.611330986 CEST	192.168.2.6	8.8.8.8	0x68f5	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:43.429347038 CEST	192.168.2.6	8.8.8.8	0x5ad6	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:50.458369017 CEST	192.168.2.6	8.8.8.8	0x33db	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:57.546703100 CEST	192.168.2.6	8.8.8.8	0xebf2	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:19:04.653218031 CEST	192.168.2.6	8.8.8.8	0xb789	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)
Jun 9, 2021 10:19:11.520154953 CEST	192.168.2.6	8.8.8.8	0xc67e	Standard query (0)	ifybest85f ff.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 10:17:53.269629002 CEST	8.8.8.8	192.168.2.6	0x288e	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:00.261193037 CEST	8.8.8.8	192.168.2.6	0xcc42	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:07.336222887 CEST	8.8.8.8	192.168.2.6	0x7ae	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:14.277889967 CEST	8.8.8.8	192.168.2.6	0x4293	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:21.331211090 CEST	8.8.8.8	192.168.2.6	0x1198	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:28.538165092 CEST	8.8.8.8	192.168.2.6	0x5b7e	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:35.654213905 CEST	8.8.8.8	192.168.2.6	0x68f5	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:43.472330093 CEST	8.8.8.8	192.168.2.6	0x5ad6	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:50.504792929 CEST	8.8.8.8	192.168.2.6	0x33db	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:18:57.590898037 CEST	8.8.8.8	192.168.2.6	0xebf2	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)
Jun 9, 2021 10:19:04.696090937 CEST	8.8.8.8	192.168.2.6	0xb789	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 10:19:11.564773083 CEST	8.8.8.8	192.168.2.6	0xc67e	No error (0)	ifybest85f ff.ddns.net		194.5.98.23	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: payment invoice.exe PID: 6660 Parent PID: 5984

General

Start time:	10:17:04
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\payment invoice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\payment invoice.exe'
Imagebase:	0xec0000
File size:	1043456 bytes
MD5 hash:	845D5DC8393BF7652F744E7FA7DFB3C3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.471352277.00000000043E9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.471352277.00000000043E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.471352277.00000000043E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.468007470.00000000033E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.471722292.0000000004589000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.471722292.0000000004589000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.471722292.0000000004589000.00000004.00000001.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: 6332 Parent PID: 6660

General

Start time:	10:17:47
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GotewYBrdNy' /XML 'C:\Users\user\AppData\Local\Temp\tmpC705.tmp'
Imagebase:	0xed0000
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: 6320 Parent PID: 6332

General

Start time:	10:17:47
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: payment invoice.exe PID: 6568 Parent PID: 6660

General

Start time:	10:17:48
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\payment invoice.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x5c0000
File size:	1043456 bytes
MD5 hash:	845D5DC8393BF7652F744E7FA7DFB3C3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

0000000B.00000000.464661919.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.464661919.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.464661919.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.646691613.0000000003AB7000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.643057638.0000000002A61000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.648627188.0000000005470000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.648627188.0000000005470000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.648627188.0000000005470000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.649963116.0000000006C40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.649963116.0000000006C40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650509970.0000000006FA0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650509970.0000000006FA0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650188515.0000000006F20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650188515.0000000006F20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.643361981.0000000002ACC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.640367723.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.640367723.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.640367723.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650157575.0000000006F10000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650157575.0000000006F10000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.648469077.0000000005280000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.648469077.0000000005280000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.646977313.0000000003C89000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650009265.0000000006C50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650009265.0000000006C50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650292848.0000000006F50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650292848.0000000006F50000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650225160.0000000006F30000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650225160.0000000006F30000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650482817.0000000006F90000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source:

	0000000B.00000002.650482817.0000000006F90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650261294.0000000006F40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650261294.0000000006F40000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650601624.0000000006FE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650601624.0000000006FE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000000.464294989.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000000.464294989.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000000.464294989.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650324913.0000000006F60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650324913.0000000006F60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.647259512.0000000003E25000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000B.00000002.650370900.0000000006F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000B.00000002.650370900.0000000006F70000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 408 Parent PID: 6568

General

Start time:	10:17:50
Start date:	09/06/2021
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\tmpD79F.tmp'
Imagebase:	0xed0000
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: 4648 Parent PID: 408

General

Start time:	10:17:51
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: payment invoice.exe PID: 976 Parent PID: 936

General

Start time:	10:17:52
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\payment invoice.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\payment invoice.exe' 0
Imagebase:	0x5e0000
File size:	1043456 bytes
MD5 hash:	845D5DC8393BF7652F744E7FA7DFB3C3
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: 00000010.00000002.572013366.0000000003A79000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.572013366.0000000003A79000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.572013366.0000000003A79000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000010.00000002.572296320.0000000003C19000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.572296320.0000000003C19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.572296320.0000000003C19000.00000004.00000001.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: 1688 Parent PID: 976

General

Start time:	10:18:30
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\GotewYBrdNy' /XML 'C:\Users\user\AppData\Local\Temp\tmp70E1.tmp'
Imagebase:	0xed0000
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: 6236 Parent PID: 1688

General

Start time:	10:18:32
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: payment invoice.exe PID: 6504 Parent PID: 976

General

Start time:	10:18:35
Start date:	09/06/2021
Path:	C:\Users\user\Desktop\payment invoice.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x5e0000
File size:	1043456 bytes
MD5 hash:	845D5DC8393BF7652F744E7FA7DFB3C3
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: 00000019.00000002.583033068.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.583033068.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.583033068.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000000.565709564.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000000.565709564.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000000.565709564.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000019.00000000.565209110.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000000.565209110.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000000.565209110.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.585683848.0000000003AA9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.585683848.0000000003AA9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000019.00000002.585357177.0000000002AA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000019.00000002.585357177.0000000002AA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis

