ID: 452642
Sample Name: R6093846s-Invoice-Receipt.exe
Cookbook: default.jbs
Time: 17:14:21
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

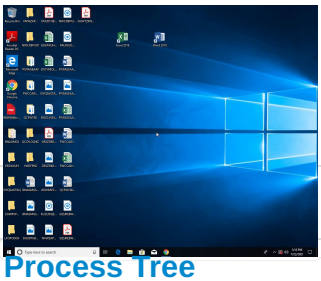
Windows Analysis Report R6093846s-Invoice-Receipt.exe

Overview

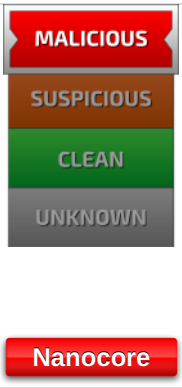
General Information

Sample Name:	R6093846s-Invoice-Receipt.exe
Analysis ID:	452642
MD5:	cd0645cb78b55f0..
SHA1:	f5221832b2b4b73.
SHA256:	5b618273e08f4e9.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

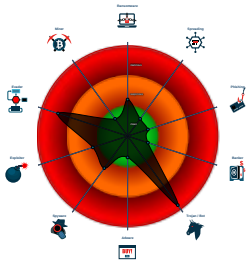


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Snort IDS alert for network traffic (e.…
- 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**
- R6093846s-Invoice-Receipt.exe (PID: 5520 cmdline: 'C:\Users\user\Desktop\R6093846s-Invoice-Receipt.exe' MD5: CD0645CB78B55F0BABBDBC4D51F23BD8)
  - schtasks.exe (PID: 5288 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UALCBPTejUQxQ' /XML 'C:\Users\user\AppData\Local\Temp\tmpCCAD.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5812 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6204 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
  - RegSvcs.exe (PID: 6232 cmdline: {path} MD5: 2867A3817C9245F7CF518524DFD18F28)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f8dffc54-5ec5-4013-9de8-d8d85368",
  "Group": "CODEDBASE",
  "Domain1": "omaprilcode.duckdns.org",
  "Domain2": "omaprilcode.duckdns.org",
  "Port": 8090,
  "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
00000014.00000002.485019554.0000000006B1 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
00000014.00000002.485019554.0000000006B1 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b99:$x2: NanoCore.ClientPluginHost • 0x6bce:$s4: PipeCreated • 0x5b86:$s5: IClientLoggingHost
00000014.00000002.484978078.0000000006AF 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
00000014.00000002.484978078.0000000006AF 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
00000014.00000002.483826250.000000000544 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 45 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
20.2.RegSvcs.exe.6b30000.32.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x170b:$x1: NanoCore.ClientPluginHost • 0x1725:$x2: IClientNetworkHost
20.2.RegSvcs.exe.6b30000.32.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x170b:$x2: NanoCore.ClientPluginHost • 0x34b6:$s4: PipeCreated • 0x16f8:$s5: IClientLoggingHost
20.2.RegSvcs.exe.6190000.23.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
20.2.RegSvcs.exe.6190000.23.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
20.2.RegSvcs.exe.6a80000.24.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
Click to see the 114 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

Jbx 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:

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:

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

Malware Analysis System Evasion:

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

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

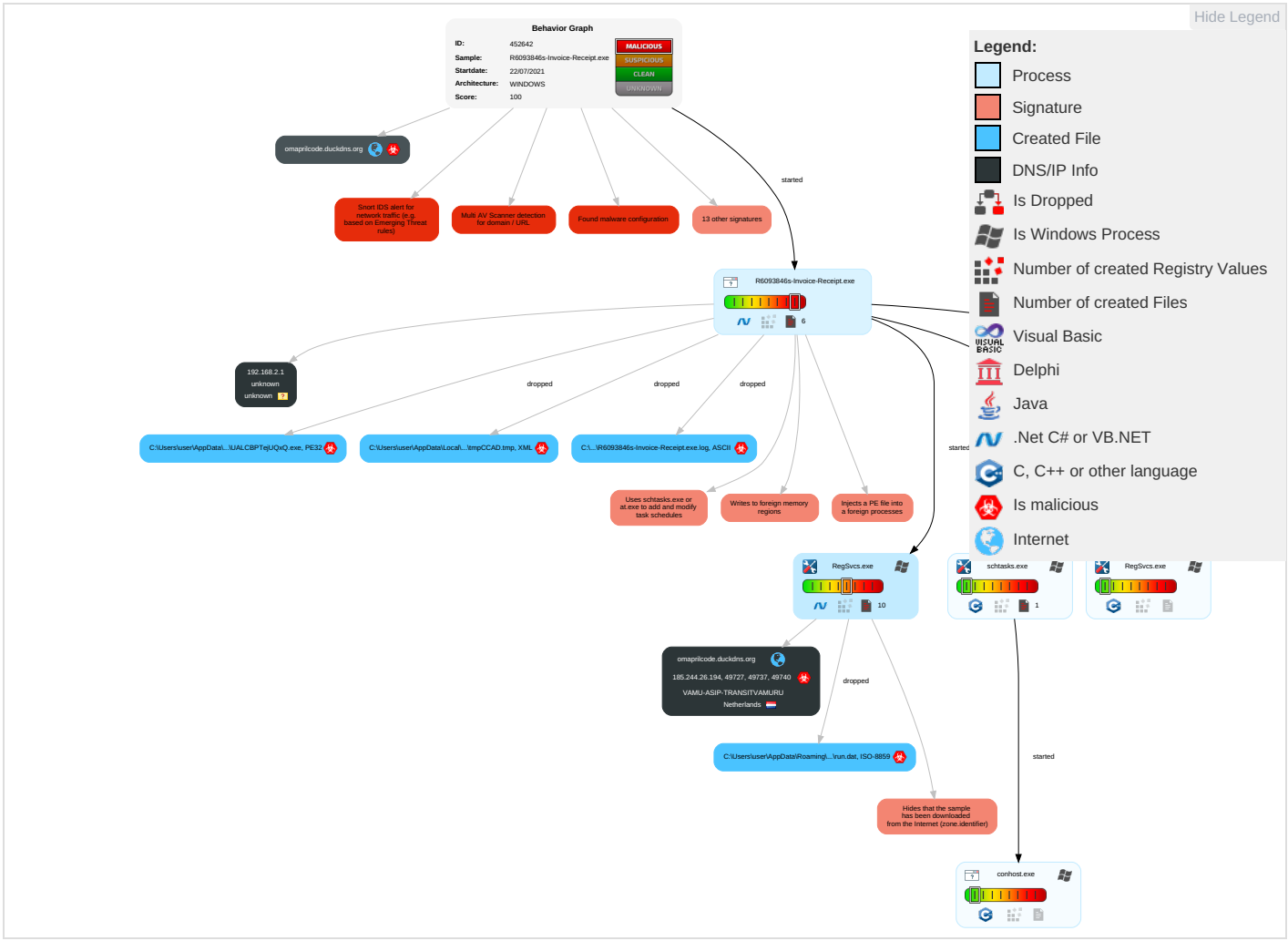
Detected Nanocore Rat

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

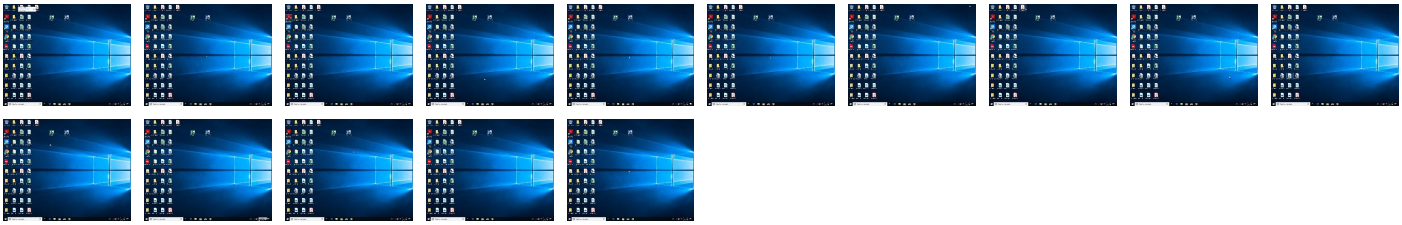
Behavior Graph



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
R6093846s-Invoice-Receipt.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
R6093846s-Invoice-Receipt.exe	100%	Joe Sandbox ML		

Dropped Files

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

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.RegSvcs.exe.5b90000.20.unpack	100%	Avira	TR/NanoCore.fadte		Download File
20.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
omaprilcode.duckdns.org	9%	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	
omaprilcode.duckdns.org	9%	Virustotal		Browse
omaprilcode.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.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.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	
http://www.sandoll.co.kr	0%	URL Reputation	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.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.zhongyicts.com.cn	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
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.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
omaprilcode.duckdns.org	185.244.26.194	true	true	• 9%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
omaprilcode.duckdns.org	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.26.194	omaprilcode.duckdns.org	Netherlands		47158	VAMU-ASIP-TRANSITVAMURU	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452642
Start date:	22.07.2021
Start time:	17:14:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 24s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	R6093846s-Invoice-Receipt.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/8@12/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.7% (good quality ratio 1.2%) • Quality average: 49.6% • Quality standard deviation: 36.4%
HCA Information:	• Successful, ratio: 99% • 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
17:15:49	API Interceptor	1x Sleep call for process: R6093846s-Invoice-Receipt.exe modified
17:15:55	API Interceptor	656x Sleep call for process: RegSvcs.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.244.26.194	DHL STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
omaprilcode.duckdns.org	ANNA-INVOICE-4725434.EXE	Get hash	malicious	Browse	• 79.134.225.6
	Victoria-Invoice-62541323.exe	Get hash	malicious	Browse	• 79.134.225.6
	Aurora-Invoice-9383736.exe	Get hash	malicious	Browse	• 79.134.225.6
	Madison-Invoice-6220917.exe	Get hash	malicious	Browse	• 79.134.225.6
	4N92zkeMjL.exe	Get hash	malicious	Browse	• 185.244.26.199
	V31802166Invoice.exe	Get hash	malicious	Browse	• 185.244.26.199
	CgzObSR6MI.exe	Get hash	malicious	Browse	• 79.134.225.9
	dautkyNrlD.exe	Get hash	malicious	Browse	• 79.134.225.9
	H538065217Invoice.exe	Get hash	malicious	Browse	• 79.134.225.9
	v4nJnRl1gt.exe	Get hash	malicious	Browse	• 79.134.225.9
	524241363INV0ICE.exe	Get hash	malicious	Browse	• 194.5.97.75
	y3t4g48gj6_PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.75
	y3t4g48gj6_PAYMENT.exe	Get hash	malicious	Browse	• 194.5.97.75
	IPUt7Nr2CH.exe	Get hash	malicious	Browse	• 194.5.97.75
	q19CDiK5TD.exe	Get hash	malicious	Browse	• 194.5.97.75

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VAMU-ASIP-TRANSITVAMURU	Swift_Fattura_0093320128_.exe	Get hash	malicious	Browse	• 185.244.26.218
	cargo detail.vbs	Get hash	malicious	Browse	• 185.244.26.213
	MFN0QBsVmm.exe	Get hash	malicious	Browse	• 185.244.26.199
	Purchase#Order20880.pdf.exe	Get hash	malicious	Browse	• 185.244.26.198
	Beatrice-Invoice-94873.exe	Get hash	malicious	Browse	• 185.244.26.199
	EVOREC - PO FH87565635456,pdf.exe	Get hash	malicious	Browse	• 185.244.26.196
	Pay014_Screenshot.exe	Get hash	malicious	Browse	• 185.244.26.199
	OIT-999-0021-21-00.vbs	Get hash	malicious	Browse	• 185.244.26.213

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	4N92zkeMjL.exe	Get hash	malicious	Browse	• 185.244.26.199
	V31802166Invoice.exe	Get hash	malicious	Browse	• 185.244.26.199
	jq9H4Yk8Uy.exe	Get hash	malicious	Browse	• 185.244.26.233
	Agency instructions.exe	Get hash	malicious	Browse	• 185.244.26.244
	ACS Leasing ACMI Details.vbs	Get hash	malicious	Browse	• 185.244.26.187
	TNT AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	• 185.244.26.237
	FIR.SCR.exe	Get hash	malicious	Browse	• 185.244.26.199
	Payment_Advice_Summary_06102021.vbs	Get hash	malicious	Browse	• 185.244.26.242
	fac.jar	Get hash	malicious	Browse	• 185.244.26.223
	PaymentDetails.exe	Get hash	malicious	Browse	• 185.244.26.234
	fature.jar	Get hash	malicious	Browse	• 185.244.26.223
	May 31st, ROSI-AOP Incident Report Details.vbs	Get hash	malicious	Browse	• 185.244.26.202

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\R6093846s-Invoice-Receipt.exe.log

Process:	C:\Users\user\Desktop\R6093846s-Invoice-Receipt.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\tmpCCAD.tmp

Process:	C:\Users\user\Desktop\R6093846s-Invoice-Receipt.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.201350821712482
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGmOtn:cbh47TlNQ//rydbz9I3YODOLNdq38J
MD5:	10825A068F66AFA5B707A7B3CDAB7FFF
SHA1:	2DD947530450B2144FA27C0947F8A3CC1088E075
SHA-256:	AF1419ABF53B8CC7904C4909ACB750191BC45C248C266D22EB3C542F3D8B9C5B
SHA-512:	652A2A58803070C30F2F88610889858EC1ECF50099CF627345A97AB80AB66004F08D9B5B5F3AEF62954997332F793E4043C33E260B50F74B808D5C91BC03D44C
Malicious:	**true**
Reputation:	low

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

Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Pri ncipal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatte ries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.109925499344649
Encrypted:	false
SSDEEP:	48:IkXEUg6ikXEUg6ikXEUg6ikXEUg6ikXEUg6ikXEUg6Z:06y6y6y6y6y6Z
MD5:	DF9DF69B9BDF9E9F14ACBA7F6AAA0439
SHA1:	F69C499EA98CB3B3FC303A8C19017F150D2FDAA1
SHA-256:	172CAF6D0566CCDAD43210FC178D55B2D12F18070F4978B27AFBE2EECB904239
SHA-512:	CBC09050EECA7053F9EE7E1E744155F2E3A7A9571C06C773B1BD7FFCCC0D2572957EDB57BBC7AD2E37C180D9CB34E306EF32CE417530386FBCC5921600E7F3 C0
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....`*kZ..JR<..e.8....z...O......f..m.PQ>Y...}.....K.,Kl..G.....qA..#.w.&..7m..B.I.....in.. <5J....z).H?....6..*2Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....`*kZ..JR<..e.8....z...O......f..m.PQ>Y...}.....K.,Kl..G. ....qA..#.w.&..7m..B.I.....in..<5J....z).H?....6..*2Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....`*kZ..JR<..e.8....z...O......f..m.P Q>Y...}.....K.,Kl..G.....qA..#.w.&..7m..B.I.....in..<5J....z).H?....6..*2Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....`*kZ ..JR<..e.8....z...O......f..m.PQ>Y...}.....K.,Kl..G.....qA..#.w.&..7m..B.I.....in..<5J....z).H?....6..*2Gj.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:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Pno8:vo8
MD5:	87A19E60362ADB0A4C4DEDA315D07F62
SHA1:	6340BAD06709D73A2D2946AC49CB5FC77B1E4DA7
SHA-256:	548F2F89D08DD063284AA4FEA0BE342B4BF8C1516613EA3DC945C294DE8816D8
SHA-512:	F2EF91AEEC6851000DB7A05D7B678BE6C5A15712D0684165D2665A135F3D4FCAF348934946F1F1766F5DA14E4613AA115D713685B243E12C30B125FCE47462F6
Malicious:	**true**
Reputation:	low
Preview:	?!..oM.H

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Preview:	9iH...}Z.4..f..J".C;"a

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1: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:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	data
Category:	dropped
Size (bytes):	317088
Entropy (8bit):	**7.999536411743182**
Encrypted:	**true**
SSDEEP:	6144:cSSJh0WiGAFfbnrQk7EJa7yflloAWFNriVBkZCCsF:QhgZJ7yfToAyiz3F
MD5:	6AB7A5BD77B3380B3DAC6164123D58C8
SHA1:	1732E82902857F97E49541719EA46CFB88FCA68B
SHA-256:	B89A2604B568E5D5435CE1885752739E481E83C08063DEA8FBC5CF271C0BA6D7
SHA-512:	DDCF3CBD63D43A0E4115E77DA62D6E94199EBB1CE836A69ADBC1CA3DB6AB0D3CDFC7EC1BD495AB93286CC52223F371ED60D36BC25547E79901CD8751B10D7CC
Malicious:	false
Preview:	z.L*Y9.7.X..~Y...q..0y....5.1e+6..d;.....i.....pk...&u..x.W1_.B.....ZP.....n...@u.uC8.o...ZX:K.C..E.S..pm.a....$.....0=H...@....n..AFi..F...H\..d..,..R@....c.{.$.@....:..>.}W..IN.....PN(..._.\..~.Z.....N..8:i.9.7.`.s.<.IX."?....{Mi..o.....M*...#]...!L .Ua_.7..D.XB.a;MP.....a..?.RQ..ni..i..z...h..R.VW^7^.i.....T/..eh.....?.j.....H..~...X.I%..8..tP...(.t>H+.s.t.w..(. ..v..!.q1+C.Z.z.vgx.'4..C..!.x.Ez.-..FR.....E..A$L.....=.Q[..)_.5c..E.~s#.{.....".a:...&:.Ye.....xu.V..v%;...FT0*..0.e...n.ss.. .,....%....0...iI.."......ira8..../.Wi.+[\....1.8.....t(.\,.$b.*z...,_..;.....M/=...}.?.....%....C<v+o...W.v..Q..H.zh).@n]....!uBY.<y9.....].fX..:(?.3..0....$.< "-.....f.m.j.+#.d7Xf.y.-C.....94}..a..S>....~)..%...?.....WI.'.hNf..UW.H.Qu.{Ns.-.....m".I.....aB4.%".....>.e.d.7...b'.I....._{..9...'.!s..P.g].e.lL).0~.V..!..\y.'..hp.u6....n.*.w.}.....P0.....3%..*=X]...`j...1.{<....NM.}t..".'..'..U.{.

C:\Users\user\AppData\Roaming\UALCBPTejUQxQ.exe	
Process:	C:\Users\user\Desktop\R6093846s-Invoice-Receipt.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	896000
Entropy (8bit):	7.28733637902053
Encrypted:	false
SSDEEP:	12288:uhdsjoEa0P0ug8+KpRJIwOauaExsH+XViPUN9AuTcxNzVD7+xQipP5r:2dsjT/zga3Ju7a+S+XViPUNiuY7Ripp
MD5:	CD0645CB78B55F0BABBDBC4D51F23BD8
SHA1:	F5221832B2B4B7338BC21E42F7E2C983D82DBDF4
SHA-256:	5B618273E08F4E9633EC359CFF551345D0DABF0C64DA9D3B5437D1C88C4BD226
SHA-512:	C2B8D05C73AB852FD4C425076E26F6D00F0A192D722B526809C6EFC5DF4623B445B5784D1C9E94DBE5EA84D7B5777451842EB898E5470422AA5AB362A369710D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....c.`.....0.....N.... .....@.. ..... ..@.....O..... ..... ..H.....text...T.... ..... ..`.rsrc.....@..@.reloc..... .....@..B.....0.....H.....G..t.....O .....W .3z...J...<hC.~.....H.`..z...,.....$.q.L.$..T..S...wsQ.IN[..jx....^3.w.....w.kB+ .r....6-...(...Qp;.<f....&.S.U.a2...*f..f.....,..f="....|..V...L..v9....O.grP.A..5...a.....J.h..T..+..#._..u...u .{.$..Y.....'.B..6,.c....s.....E8..w..3. .1..D.oU3=.j...._.-&.7-..l.....H..7) ..kL....G....V.....0.u.....V.^.Rk.....|.:..+...b^.k..+.]..../..q....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.28733637902053

General

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:	R6093846s-Invoice-Receipt.exe
File size:	896000
MD5:	cd0645cb78b55f0babbdbc4d51f23bd8
SHA1:	f5221832b2b4b7338bc21e42f7e2c983d82dbdf4
SHA256:	5b618273e08f4e9633ec359cff551345d0dabf0c64da9d3b5437d1c88c4bd226
SHA512:	c2b8d05c73ab852fd4c425076e26f6d00f0a192d722b526809c6efc5df4623b445b5784d1c9e94dbe5ea84d7b5777451842eb898e5470422aa5ab362a369710d
SSDEEP:	12288:uhdsjoEa0P0ug8+KpRJlwOauaExsH+XViPUN9AuTcxNzVD7+xQipP5r:2dsjT/zga3Ju7a+S+XViPUNiuY7Ripp
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....c.`.....0.....N.... ....@.. .....@.....

File Icon

Icon Hash:	1a72e2e4747a6662

Static PE Info

General

Entrypoint:	0x48f84e
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:	0x60F96389 [Thu Jul 22 12:24:41 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	0x8d854	0x8da00	False	0.869911187114	data	7.77156503233	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x90000	0x4cca8	0x4ce00	False	0.181107088415	data	5.87991492368	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xde000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
07/22/21-17:15:57.652962	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49727	8090	192.168.2.3	185.244.26.194
07/22/21-17:16:07.297979	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	8090	192.168.2.3	185.244.26.194
07/22/21-17:16:13.534653	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49740	8090	192.168.2.3	185.244.26.194
07/22/21-17:16:22.015102	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	8090	192.168.2.3	185.244.26.194
07/22/21-17:16:29.006113	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	8090	192.168.2.3	185.244.26.194
07/22/21-17:16:35.941770	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	8090	192.168.2.3	185.244.26.194
07/22/21-17:16:43.040140	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	8090	192.168.2.3	185.244.26.194
07/22/21-17:16:50.097122	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	8090	192.168.2.3	185.244.26.194
07/22/21-17:16:57.147005	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	8090	192.168.2.3	185.244.26.194
07/22/21-17:17:04.420377	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	8090	192.168.2.3	185.244.26.194
07/22/21-17:17:11.448870	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	8090	192.168.2.3	185.244.26.194
07/22/21-17:17:18.070997	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	8090	192.168.2.3	185.244.26.194

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:15:56.759084940 CEST	192.168.2.3	8.8.8.8	0xd325	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:07.048366070 CEST	192.168.2.3	8.8.8.8	0x8b3e	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:13.270433903 CEST	192.168.2.3	8.8.8.8	0xfd27	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:21.740432978 CEST	192.168.2.3	8.8.8.8	0x8bbe	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:28.626430035 CEST	192.168.2.3	8.8.8.8	0xf1e6	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:35.643198013 CEST	192.168.2.3	8.8.8.8	0xa0da	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:42.720694065 CEST	192.168.2.3	8.8.8.8	0x47df	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:49.797224045 CEST	192.168.2.3	8.8.8.8	0x365c	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:56.884917021 CEST	192.168.2.3	8.8.8.8	0xace2	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:17:04.036845922 CEST	192.168.2.3	8.8.8.8	0x22c1	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)
Jul 22, 2021 17:17:11.173968077 CEST	192.168.2.3	8.8.8.8	0x9904	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 17:17:17.807742119 CEST	192.168.2.3	8.8.8.8	0xaf5f	Standard query (0)	omaprilcode.duckdns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:15:56.923748970 CEST	8.8.8.8	192.168.2.3	0xd325	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:07.097353935 CEST	8.8.8.8	192.168.2.3	0x8b3e	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:13.327728033 CEST	8.8.8.8	192.168.2.3	0xfd27	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:21.797602892 CEST	8.8.8.8	192.168.2.3	0x8bbe	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:28.781832933 CEST	8.8.8.8	192.168.2.3	0xf1e6	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:35.703490973 CEST	8.8.8.8	192.168.2.3	0xa0da	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:42.780225992 CEST	8.8.8.8	192.168.2.3	0x47df	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:49.857126951 CEST	8.8.8.8	192.168.2.3	0x365c	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:16:56.943536043 CEST	8.8.8.8	192.168.2.3	0xace2	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:17:04.189584017 CEST	8.8.8.8	192.168.2.3	0x22c1	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:17:11.235089064 CEST	8.8.8.8	192.168.2.3	0x9904	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)
Jul 22, 2021 17:17:17.867338896 CEST	8.8.8.8	192.168.2.3	0xaf5f	No error (0)	omaprilcode.duckdns.org		185.244.26.194	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: R6093846s-Invoice-Receipt.exe PID: 5520 Parent PID: 5576

General

Start time:	17:15:09
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\R6093846s-Invoice-Receipt.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\R6093846s-Invoice-Receipt.exe'
Imagebase:	0x300000
File size:	896000 bytes
MD5 hash:	CD0645CB78B55F0BABBDBC4D51F23BD8
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: 00000000.00000002.305161176.000000000396B000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.305161176.000000000396B000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.305161176.000000000396B000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.304879840.0000000003759000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.304879840.0000000003759000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.304879840.0000000003759000.00000004.00000001.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: 5288 Parent PID: 5520

General

Start time:	17:15:50
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UALCBPTejUQxQ' /XML 'C:\Users\user\AppData\Local\Temp\tmpCCAD.tmp'
Imagebase:	0xae0000
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: 5812 Parent PID: 5288

General

Start time:	17:15:51
Start date:	22/07/2021
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: RegSvcs.exe PID: 6204 Parent PID: 5520

General

Start time:	17:15:51
Start date:	22/07/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x1b0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6232 Parent PID: 5520

General

Start time:	17:15:52
Start date:	22/07/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
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: 00000014.00000002.485019554.0000000006B10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.485019554.0000000006B10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484978078.0000000006AF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484978078.0000000006AF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.483826250.0000000005440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.483826250.0000000005440000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484104685.0000000005B90000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484104685.0000000005B90000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.484104685.0000000005B90000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.485071825.0000000006B30000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.485071825.0000000006B30000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.480562084.0000000004325000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000002.480562084.0000000004325000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.470391681.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.470391681.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000002.470391681.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484960992.0000000006AE0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484960992.0000000006AE0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.479043770.0000000003891000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000002.479043770.0000000003891000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484915497.0000000006AC0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484915497.0000000006AC0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484897789.0000000006AB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484897789.0000000006AB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.485130700.0000000006B80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.485130700.0000000006B80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.480703873.0000000004486000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000014.00000002.480703873.0000000004486000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484998886.0000000006B00000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484998886.0000000006B00000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484851372.0000000006A80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484851372.0000000006A80000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.485085026.0000000006B40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.485085026.0000000006B40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.474458367.0000000002891000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484936957.0000000006AD0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484936957.0000000006AD0000.00000004.00000001.sdmp, Author: Florian Roth

	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000014.00000002.480187851.0000000004161000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000014.00000002.480187851.0000000004161000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000014.00000002.484499149.0000000006190000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000014.00000002.484499149.0000000006190000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	high

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Disassembly

Code Analysis