Joe Sandbox Cloud BASIC

ID: 451105
Sample Name: ORDER TSA-A090621B.exe
Cookbook: default.jbs
Time: 08:34:07
Date: 20/07/2021
Version: 33.0.0 White Diamond

Table of Contents

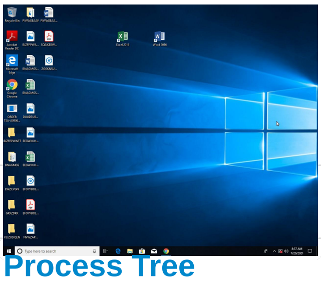
Windows Analysis Report ORDER TSA-A090621B.exe

Overview

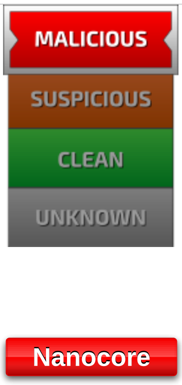
General Information

Sample Name:	ORDER TSA-A090621B.exe
Analysis ID:	451105
MD5:	f5d3b895f4109e0..
SHA1:	e4fe29023bd9af1..
SHA256:	9713a28e0645cc..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

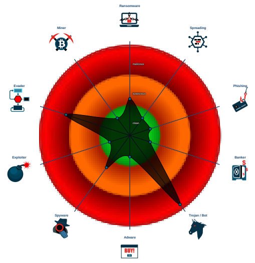


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Initial sample is a PE file and has a …
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- ORDER TSA-A090621B.exe (PID: 3980 cmdline: 'C:\Users\user\Desktop\ORDER TSA-A090621B.exe' MD5: F5D3B895F4109E09F8918FC52147D154)
  - ORDER TSA-A090621B.exe (PID: 5464 cmdline: C:\Users\user\Desktop\ORDER TSA-A090621B.exe MD5: F5D3B895F4109E09F8918FC52147D154)
  - ORDER TSA-A090621B.exe (PID: 5692 cmdline: C:\Users\user\Desktop\ORDER TSA-A090621B.exe MD5: F5D3B895F4109E09F8918FC52147D154)
- dhcpmon.exe (PID: 5228 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: F5D3B895F4109E09F8918FC52147D154)
  - dhcpmon.exe (PID: 2476 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: F5D3B895F4109E09F8918FC52147D154)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "c9622013-90b3-4810-9b2a-2fbba172",
  "Domain1": "185.140.53.253",
  "Domain2": "dedicatedlambo9.ddns.net",
  "Port": 1604,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "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
00000006.00000002.499314536.0000000006B90000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5fee:$x1: NanoCore.ClientPluginHost • 0x602b:$x2: IClientNetworkHost
00000006.00000002.499314536.0000000006B90000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5fee:$x2: NanoCore.ClientPluginHost • 0x9441:$s4: PipeCreated • 0x6018:$s5: IClientLoggingHost
00000006.00000002.500192513.0000000007710000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
00000006.00000002.500192513.0000000007710000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x8ba5:$x2: NanoCore.ClientPluginHost • 0x9b74:$s2: FileCommand • 0xe576:$s4: PipeCreated • 0x8bbf:$s5: IClientLoggingHost
00000015.00000002.396003210.00000000039E9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 46 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.2.ORDER TSA-A090621B.exe.6b00000.22.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x59eb:$x1: NanoCore.ClientPluginHost • 0x5b48:$x2: IClientNetworkHost
6.2.ORDER TSA-A090621B.exe.6b00000.22.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x59eb:$x2: NanoCore.ClientPluginHost • 0x6941:$s3: PipeExists • 0x5be1:$s4: PipeCreated • 0x5a05:$s5: IClientLoggingHost
6.2.ORDER TSA-A090621B.exe.6b20000.24.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
6.2.ORDER TSA-A090621B.exe.6b20000.24.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b99:$x2: NanoCore.ClientPluginHost • 0x6bce:$s4: PipeCreated • 0x5b86:$s5: IClientLoggingHost
6.2.ORDER TSA-A090621B.exe.65e4629.19.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
Click to see the 126 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:

- 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

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

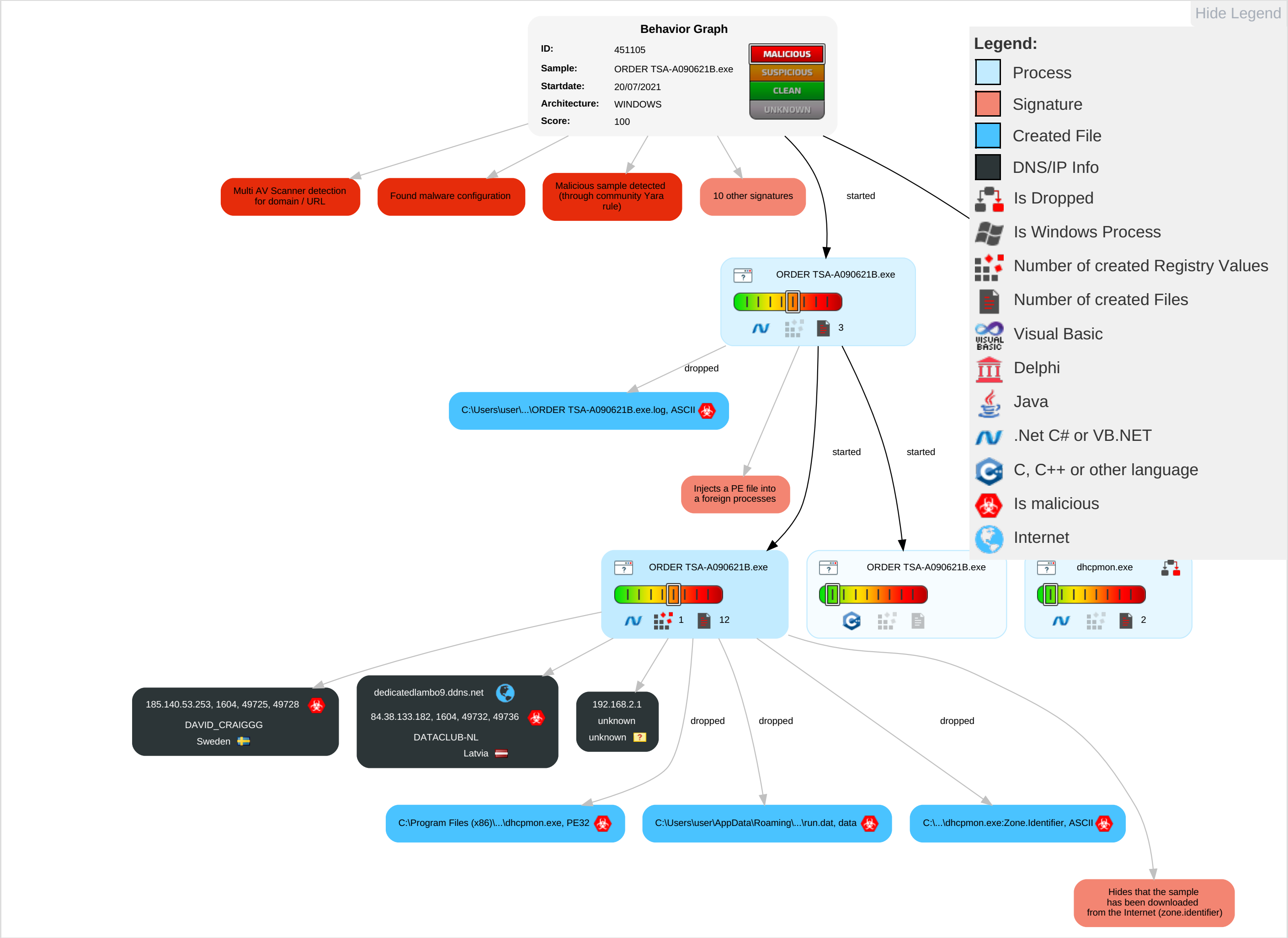
Detected Nanocore Rat

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	Path Interception	Process Injection 1 1 2	Masquerading 2	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	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	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	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	Software Packing 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	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

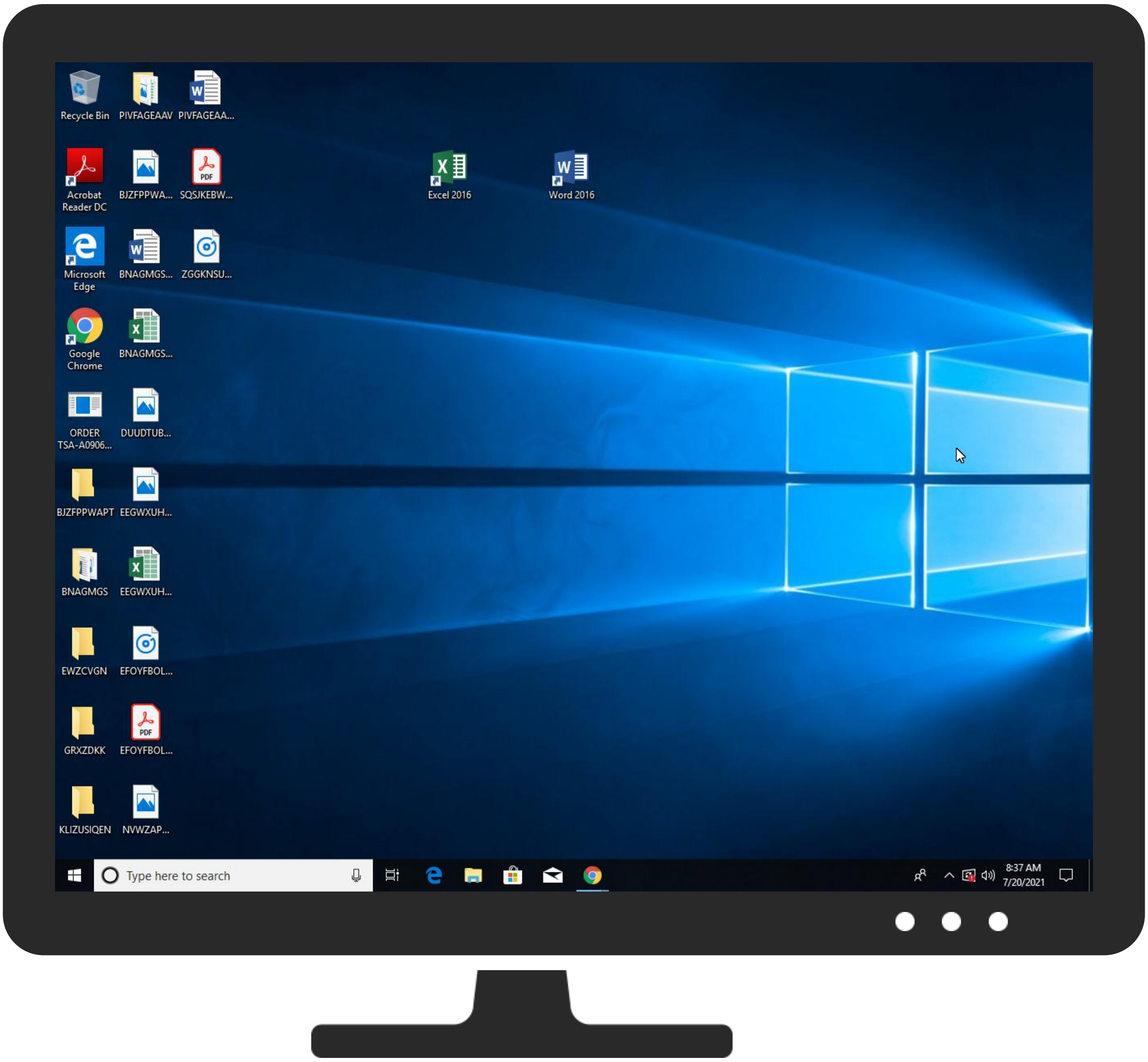
Behavior Graph



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
ORDER TSA-A090621B.exe	21%	Virustotal		Browse
ORDER TSA-A090621B.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	17%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.ORDER TSA-A090621B.exe.65e0000.18.unpack	100%	Avira	TR/NanoCore.fadte		Download File
21.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
6.2.ORDER TSA-A090621B.exe.44b8a40.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
6.2.ORDER TSA-A090621B.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
dedicatedlambo9.ddns.net	7%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
dedicatedlambo9.ddns.net	7%	Virustotal		Browse
dedicatedlambo9.ddns.net	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comdr	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.tiro.comn	0%	URL Reputation	safe	
http://www.founder.com.cn/cnU	0%	Avira URL Cloud	safe	
http://www.fontbureau.comueTF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/M	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnA	0%	Avira URL Cloud	safe	
http://www.sakkal.comx.	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.sajatypeworks.comD	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/71	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/vau	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/arge	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Y0d	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.fontbureau.comcomF	0%	URL Reputation	safe	
http://www.fontbureau.comcomF	0%	URL Reputation	safe	
http://www.fontbureau.comcomF	0%	URL Reputation	safe	
http://www.fontbureau.comonyd	0%	Avira URL Cloud	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/jp/71	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.html	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.sakkal.comd	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.urwpp.delar	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comc	0%	Avira URL Cloud	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/s	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ns.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/vnoi	0%	Avira URL Cloud	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	
185.140.53.253	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn#	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	
http://www.founder.com.cn/cnd	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dedicatedlambo9.ddns.net	84.38.133.182	true	true	• 7%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
dedicatedlambo9.ddns.net	true	• 7%, Virustotal, Browse • Avira URL Cloud: safe	unknown
185.140.53.253	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
84.38.133.182	dedicatedlambo9.ddns.net	Latvia	🇱🇻	203557	DATACLUB-NL	true
185.140.53.253	unknown	Sweden	🇸🇪	209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	451105
Start date:	20.07.2021
Start time:	08:34:07
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 33s
Hypervisor based Inspection enabled:	false
Report type:	light

Sample file name:	ORDER TSA-A090621B.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/8@12/3
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • 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
08:35:27	API Interceptor	800x Sleep call for process: ORDER TSA-A090621B.exe modified
08:35:33	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
08:36:14	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
84.38.133.182	RFQ 10 UNIT.exe	Get hash	malicious	Browse	
185.140.53.253	RFQ 10 UNIT.exe	Get hash	malicious	Browse	
	NEWORDERrefno0992883jpg.exe	Get hash	malicious	Browse	
	CompanyLicense.exe	Get hash	malicious	Browse	
	16Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	15Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	58Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	57Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	15Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	14Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	
	57Product Specifications list -Order PCT1086586 1st Video.exe	Get hash	malicious	Browse	
	56Order PCT1086586 - Project Commercial Conditions.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dedicatedlambo9.ddns.net	RFQ 10 UNIT.exe	Get hash	malicious	Browse	• 84.38.133.182

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	RFQ 10 UNIT.exe	Get hash	malicious	Browse	• 185.140.53.253
	A2CGhuioKe.exe	Get hash	malicious	Browse	• 185.244.30.28
	0kEuVjiCbh.exe	Get hash	malicious	Browse	• 185.244.30.28
	RFQ_Order WT013 - A11197322,pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	ORDER.exe	Get hash	malicious	Browse	• 185.140.53.132
	DHL_119040 receipt document,pdf.exe	Get hash	malicious	Browse	• 185.244.30.18
	Img 673t5718737.exe	Get hash	malicious	Browse	• 91.193.75.202
	Parts_Enquiry_450kr6CRT.vbs	Get hash	malicious	Browse	• 185.140.53.169
	Itemsreceipt975432907.exe	Get hash	malicious	Browse	• 185.244.30.19
	H194 #U5146#U57fa - Payment.exe	Get hash	malicious	Browse	• 185.140.53.135
	Parts-Enquiry_OYU08W0VCWRDLPA.vbs	Get hash	malicious	Browse	• 185.140.53.169
	OneDrive.exe	Get hash	malicious	Browse	• 185.140.53.194
	CVhssiltQ9.exe	Get hash	malicious	Browse	• 185.140.53.9
	rz89FRwKvB.exe	Get hash	malicious	Browse	• 185.244.30.92
	doc030WA0004-55YH701-75IMG0012.exe	Get hash	malicious	Browse	• 185.140.53.230
	Request For Quotation.xlsx	Get hash	malicious	Browse	• 185.140.53.154
	CV CREDENTIALS.exe	Get hash	malicious	Browse	• 185.140.53.8
	ARRIVAL NOTICEPDF.EXCL.exe	Get hash	malicious	Browse	• 185.140.53.142
	WeASwOPOdNuVKbq.exe	Get hash	malicious	Browse	• 185.140.53.8
	New Order# 11009947810.exe	Get hash	malicious	Browse	• 185.140.53.216
DATACLUB-NL	RFQ 10 UNIT.exe	Get hash	malicious	Browse	• 84.38.133.182
	FacebookSecurityUpdate.exe	Get hash	malicious	Browse	• 84.38.133.101
	v1hBv6A71M.exe	Get hash	malicious	Browse	• 84.38.133.24
	Standardequips_Quote.ppt	Get hash	malicious	Browse	• 185.29.11.15
	XsNgUDFxLw.exe	Get hash	malicious	Browse	• 84.38.133.117
	18Order.exe	Get hash	malicious	Browse	• 185.29.11.103
	56New Order oct 2018230090.exe	Get hash	malicious	Browse	• 185.29.11.103

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1102336
Entropy (8bit):	7.620117442134609
Encrypted:	false
SSDEEP:	24576:D0QSJpE4KrvDBbG5wOCYDr82fY+9s1q2MpSD3g:0+JG6BcICCN3
MD5:	F5D3B895F4109E09F8918FC52147D154
SHA1:	E4FE29023BD9AF1916D7C12197949DDAED424E8B
SHA-256:	9713A28E0645CC77089DFD921118DB8827DE0A8B7E8196D653DA2002646BD3CF
SHA-512:	3F3A765C18E5D2C5E39E815476B533BEFD98ADEDE73C4976A12F8B9E3BD8F5BB3B8EA995E48B4B9DEC364B82BC8C0F80E0E783C5E6DA29C293A1FDA8AEEB 5C1
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 17%
Reputation:	low

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....................P.............B.... ....@.. ....@...........@.....................................O............................ ....H............text...H.... ....`.rsrc...............................@..@.reloc....... ....@..B................$.......H...........4|..........$....L..0............(....(.........(.....o!....*.....................(".......(#......($......(%......(&....*N..(....o....('....*&..((....*.s)........s*........s+........s,........s-........*....0...........~....o.....+..*.0...........~....o/....+..*.0...........~....o0....+..*.0...........~....o1....+..*.0...........~....o2....+..*&..(3....*....0..<........~.....(4.....,!r...p.....(5...o6...s7............~.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\ORDER TSA-A090621B.exe.log

Process:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	false
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0IlC0IlC0IlC0IlC0IlC0IlC08
MD5:	0D79388CEC6619D612C2088173BB6741
SHA1:	8A312E3198009C545D0CF3254572189D29A03EA7
SHA-256:	D7D423B23D932E306F3CCB2F7A984B7036A042C007A43FD655C6B57B960BB8DF
SHA-512:	53BB3E9263DFD746E7E8159466E220E6EC9D81E9D3F0E1D191E09CD511B7EB93B0BA65D13CE0C97C652ECD0F69BB991E6B1840F961BC65003C4DD7AA93EED 13
Malicious:	false
Reputation:	moderate, very likely benign file
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\ORDER TSA-A090621B.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:7ht:tt
MD5:	A7550BD6998D4B201226569FAD19FEE2
SHA1:	9B40BDC466BCB9BD006D37E5704C428A8EA6AC7D
SHA-256:	C484DF23E31180678D28C7C68F6DAA4F721849C74613C19EEB9920CDBF544466
SHA-512:	8622EDACFC4BD5C90BD976BB008FBC142E6B6CE6326B5C27BA8D86E22527F6F055D91DC1BD67E094A3EF9951D7920B0DE600F0210A50342D1ED3D5F01288EA C
Malicious:	**true**
Preview:	.s...K.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
File Type:	data
Category:	modified
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Preview:	9iH...}Z.4..f.~a........~.~.......3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
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....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.620117442134609
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	ORDER TSA-A090621B.exe
File size:	1102336
MD5:	f5d3b895f4109e09f8918fc52147d154
SHA1:	e4fe29023bd9af1916d7c12197949ddaed424e8b
SHA256:	9713a28e0645cc77089dfd921118db8827de0a8b7e8196 d653da2002646bd3cf
SHA512:	3f3a765c18e5d2c5e39e815476b533befd98adede73c497 6a12f8b9e3bd8f5bb3b8ea995e48b4b9dec364b82bc8c0f 80e0e783c5e6da29c293a1fda8aeeb95c1
SSDEEP:	24576:D0QSJpE4KrvDBbG5wOCYDr82fY+9s1q2MpSD3g:0+JG6BcICCN3
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L..... ................P.............B.... ....@.. ....@......... ...@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x50e942
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:	0xD09DABD0 [Thu Nov 28 04:34:24 2080 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4

General

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	0x10c948	0x10ca00	False	0.77032467863	data	7.62512581288	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x110000	0x3a8	0x400	False	0.3740234375	data	2.91950610469	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x112000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2021 08:35:51.531042099 CEST	192.168.2.3	8.8.8.8	0x461b	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:35:59.546921968 CEST	192.168.2.3	8.8.8.8	0xa3c3	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:04.778085947 CEST	192.168.2.3	8.8.8.8	0xdff9	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:11.737570047 CEST	192.168.2.3	8.8.8.8	0x88a6	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:19.305597067 CEST	192.168.2.3	8.8.8.8	0x711b	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:25.514846087 CEST	192.168.2.3	8.8.8.8	0x676f	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:32.455975056 CEST	192.168.2.3	8.8.8.8	0x237b	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:38.505142927 CEST	192.168.2.3	8.8.8.8	0xcdcf	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:45.567162037 CEST	192.168.2.3	8.8.8.8	0xa1e0	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:51.571012974 CEST	192.168.2.3	8.8.8.8	0xf34c	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:57.688997030 CEST	192.168.2.3	8.8.8.8	0xd032	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 20, 2021 08:37:04.547127008 CEST	192.168.2.3	8.8.8.8	0xb17	Standard query (0)	dedicatedlambo9.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 20, 2021 08:35:51.592425108 CEST	8.8.8.8	192.168.2.3	0x461b	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:35:59.605354071 CEST	8.8.8.8	192.168.2.3	0xa3c3	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:04.838644981 CEST	8.8.8.8	192.168.2.3	0xdff9	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:11.796391010 CEST	8.8.8.8	192.168.2.3	0x88a6	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:19.363178015 CEST	8.8.8.8	192.168.2.3	0x711b	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:25.573158979 CEST	8.8.8.8	192.168.2.3	0x676f	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:32.516514063 CEST	8.8.8.8	192.168.2.3	0x237b	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:38.567308903 CEST	8.8.8.8	192.168.2.3	0xcdcf	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:45.625282049 CEST	8.8.8.8	192.168.2.3	0xa1e0	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:51.632529020 CEST	8.8.8.8	192.168.2.3	0xf34c	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:36:57.746087074 CEST	8.8.8.8	192.168.2.3	0xd032	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)
Jul 20, 2021 08:37:04.605415106 CEST	8.8.8.8	192.168.2.3	0xb17	No error (0)	dedicatedlambo9.ddns.net		84.38.133.182	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: ORDER TSA-A090621B.exe PID: 3980 Parent PID: 5584

General

Start time:	08:34:59
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe

Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ORDER TSA-A090621B.exe'
Imagebase:	0xaa0000
File size:	1102336 bytes
MD5 hash:	F5D3B895F4109E09F8918FC52147D154
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: ORDER TSA-A090621B.exe PID: 5464 Parent PID: 3980

General

Start time:	08:35:28
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
Imagebase:	0x60000
File size:	1102336 bytes
MD5 hash:	F5D3B895F4109E09F8918FC52147D154
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: ORDER TSA-A090621B.exe PID: 5692 Parent PID: 3980

General

Start time:	08:35:29
Start date:	20/07/2021
Path:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\ORDER TSA-A090621B.exe
Imagebase:	0xfb0000
File size:	1102336 bytes
MD5 hash:	F5D3B895F4109E09F8918FC52147D154
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: 00000006.00000002.499314536.0000000006B90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.499314536.0000000006B90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.500192513.0000000007710000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.500192513.0000000007710000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source:

00000006.00000002.500525648.0000000007C60000.00000004.00000001.sdmp, Author: Florian Roth

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.500525648.0000000007C60000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000006.00000002.495158734.00000000045F7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.499144017.0000000006AF0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.499144017.0000000006AF0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000006.00000002.495469070.000000000478F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.499169439.0000000006B00000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.499169439.0000000006B00000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.500549861.0000000007C70000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.500549861.0000000007C70000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.498290659.0000000005BB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.498290659.0000000005BB0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000006.00000002.495497287.00000000047A6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.499236783.0000000006B40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.499236783.0000000006B40000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.499201133.0000000006B20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.499201133.0000000006B20000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000006.00000002.489488042.00000000034CA000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.500174587.0000000007700000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.500174587.0000000007700000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.498755747.00000000065E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.498755747.00000000065E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.498755747.00000000065E0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.499185267.0000000006B10000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.499185267.0000000006B10000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.482529229.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.482529229.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000006.00000002.482529229.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.500371325.00000000079D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.500371325.00000000079D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.494838294.00000000044A5000.00000004.00000001.sdmp, Author:

	Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.489008599.0000000003451000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.499269257.0000000006B60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.499269257.0000000006B60000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: dhcpmon.exe PID: 5228 Parent PID: 3388

General

Start time:	08:35:42
Start date:	20/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xcf0000
File size:	1102336 bytes
MD5 hash:	F5D3B895F4109E09F8918FC52147D154
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 17%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: dhcpmon.exe PID: 2476 Parent PID: 5228

General

Start time:	08:36:15
Start date:	20/07/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0x620000
File size:	1102336 bytes
MD5 hash:	F5D3B895F4109E09F8918FC52147D154
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.396003210.00000000039E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.396003210.00000000039E9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000015.00000002.394406077.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.394406077.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.394406077.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.395871359.00000000029E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.395871359.00000000029E1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis