ID: 528510
Sample Name: SK TAX INV.exe
Cookbook: default.jbs
Time: 11:55:18
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SK TAX INV.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: NanoCore 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
AV Detection: 6
E-Banking Fraud: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Jbx Signature Overview 6
AV Detection: 6
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 8
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 15
Sections 15
Resources 15
Imports 15
Version Infos 15
Network Behavior 15
Snort IDS Alerts 15
Network Port Distribution 16
TCP Packets 16
UDP Packets 16
DNS Queries 16
DNS Answers 17
Code Manipulations 18
Statistics 18

Behavior 18
System Behavior 18
Analysis Process: SK TAX INV.exe PID: 3980 Parent PID: 5296 18
General 18
File Activities 19
File Created 19
File Written 19
File Read 19
Analysis Process: SK TAX INV.exe PID: 6636 Parent PID: 3980 19
General 19
File Activities 20
File Created 20
File Deleted 20
File Written 20
File Read 20
Registry Activities 20
Key Value Created 20
Analysis Process: dhcpmon.exe PID: 6980 Parent PID: 3424 20
General 20
Disassembly 21
Code Analysis 21

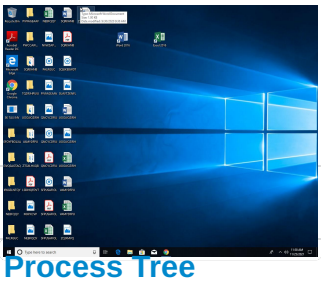
Windows Analysis Report SK TAX INV.exe

Overview

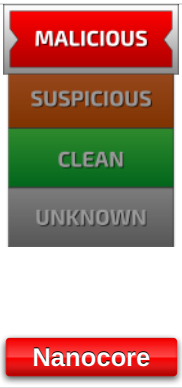
General Information

Sample Name:	SK TAX INV.exe
Analysis ID:	528510
MD5:	c2ee32f9d7de6b0.
SHA1:	d4455ac7ec0c49…
SHA256:	84b9fef1f2c0dd3…
Tags:	exe Invoice
Infos:	

Most interesting Screenshot:



Detection



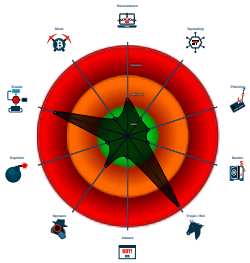
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- SK TAX INV.exe (PID: 3980 cmdline: "C:\Users\user\Desktop\SK TAX INV.exe" MD5: C2EE32F9D7DE6B05472CEDA926FD0A6F)
  - SK TAX INV.exe (PID: 6636 cmdline: C:\Users\user\Desktop\SK TAX INV.exe MD5: C2EE32F9D7DE6B05472CEDA926FD0A6F)
- dhcpmon.exe (PID: 6980 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: C2EE32F9D7DE6B05472CEDA926FD0A6F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "f4157c11-54e5-4893-8a60-6856b847",
  "Group": "Default",
  "Domain1": "dera31.ddns.net",
  "Domain2": "195.133.18.211",
  "Port": 1187,
  "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
00000003.00000000.665221730.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000003.00000000.665221730.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000003.00000000.665221730.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000003.00000000.665589656.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000003.00000000.665589656.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.SK TAX INV.exe.400000.10.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
3.0.SK TAX INV.exe.400000.10.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
3.0.SK TAX INV.exe.400000.10.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.0.SK TAX INV.exe.400000.10.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
3.0.SK TAX INV.exe.400000.8.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 31 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 submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

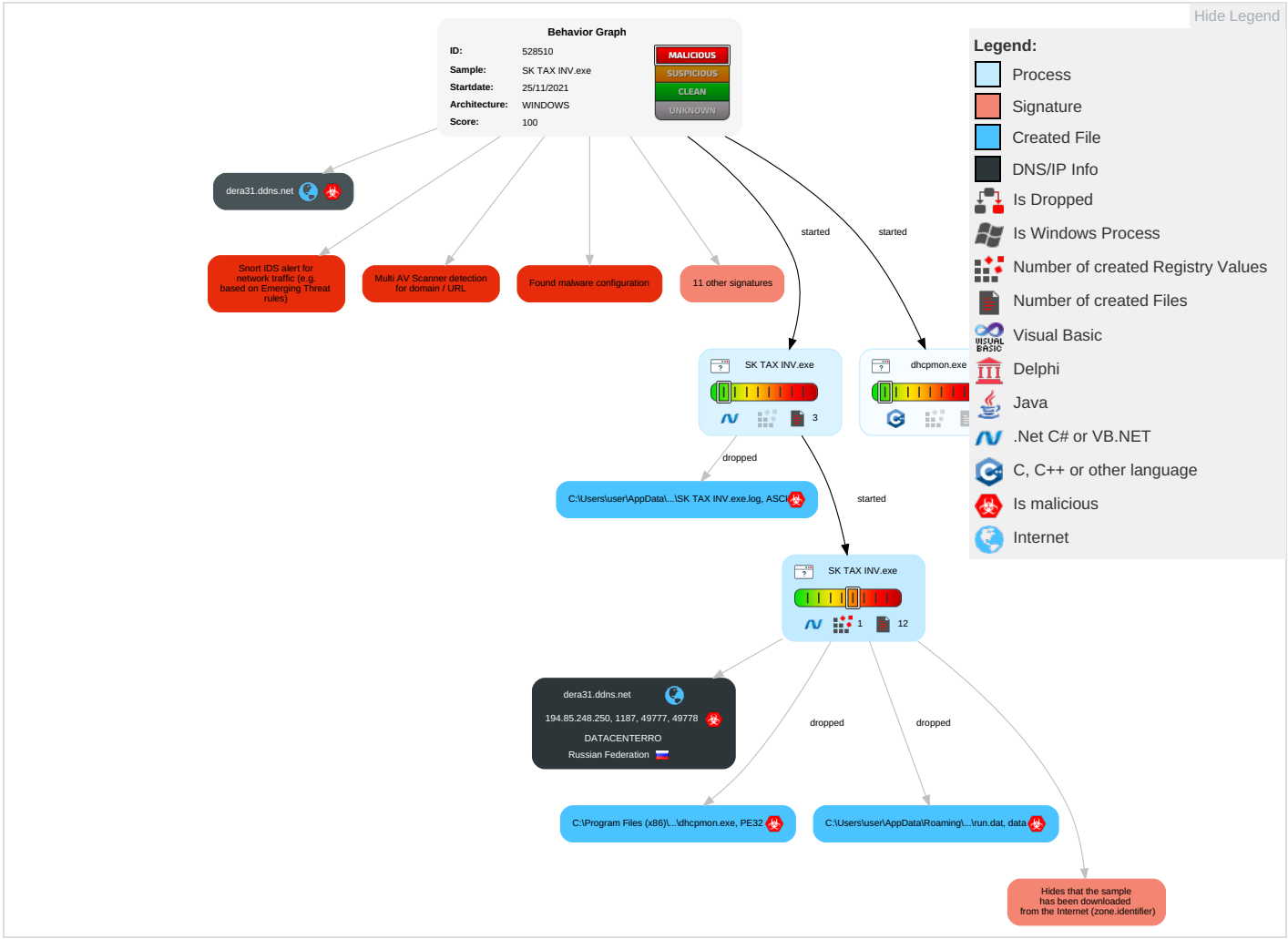
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1 1	Masquerading 2	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdr Insecure Network Commun
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Car Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 1	Manipula Device Commur
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial o Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue V Access I
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocol

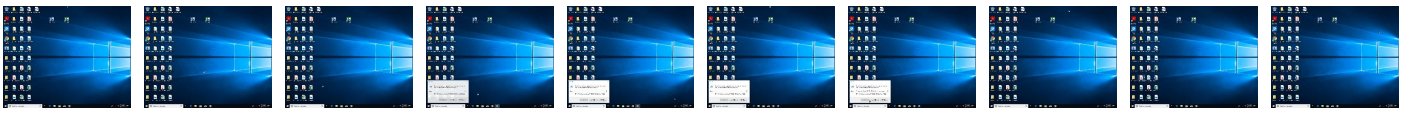
Behavior Graph



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
SK TAX INV.exe	18%	Virustotal		Browse
SK TAX INV.exe	11%	ReversingLabs	Win32.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	18%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	20%	ReversingLabs	Win32.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.SK TAX INV.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.SK TAX INV.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.SK TAX INV.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.SK TAX INV.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.SK TAX INV.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
dera31.ddns.net	6%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
dera31.ddns.net	6%	Virustotal		Browse
dera31.ddns.net	0%	Avira URL Cloud	safe	
195.133.18.211	6%	Virustotal		Browse
195.133.18.211	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
dera31.ddns.net	194.85.248.250	true	true	• 6%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
dera31.ddns.net	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown
195.133.18.211	true	• 6%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.85.248.250	dera31.ddns.net	Russian Federation		35478	DATACENTERRO	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528510
Start date:	25.11.2021
Start time:	11:55:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SK TAX INV.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:	17
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@4/7@20/1
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
11:56:12	API Interceptor	1029x Sleep call for process: SK TAX INV.exe modified
11:56:20	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
194.85.248.250	CV.exe	Get hash	malicious	Browse	
	INV.exe	Get hash	malicious	Browse	
	CV.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
dera31.ddns.net	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	INV.exe	Get hash	malicious	Browse	• 194.85.248.250
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	circular_11_17_21.exe	Get hash	malicious	Browse	• 195.133.18.211
	Bank Report.exe	Get hash	malicious	Browse	• 195.133.18.211
	cliff.kuhfeldt's CV.exe	Get hash	malicious	Browse	• 195.133.18.211
	Jessica Ohnesorge'CV.exe	Get hash	malicious	Browse	• 195.133.18.211
	Change Of Registration Form.exe	Get hash	malicious	Browse	• 195.133.18.211
	Payment invoice.exe	Get hash	malicious	Browse	• 195.133.18.211
	Wire Transfer Slip.exe	Get hash	malicious	Browse	• 195.133.18.211
	Advise.exe	Get hash	malicious	Browse	• 195.133.18.211
	Bank Report.exe	Get hash	malicious	Browse	• 195.133.18.211
	N5HlpHINh2.exe	Get hash	malicious	Browse	• 195.133.18.211
	BL draft.exe	Get hash	malicious	Browse	• 195.133.18.211

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DATACENTERRO	xA7ry4Ewuk.exe	Get hash	malicious	Browse	• 194.85.248.167
	Sales Pro forma invoice_SO0005303101427.docx	Get hash	malicious	Browse	• 194.85.248.219
	Statement from QNB.exe	Get hash	malicious	Browse	• 194.85.248.156
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	INV.exe	Get hash	malicious	Browse	• 194.85.248.250
	CV.exe	Get hash	malicious	Browse	• 194.85.248.250
	TMR590241368.exe	Get hash	malicious	Browse	• 194.85.248.115
	vIyyHkRXJn	Get hash	malicious	Browse	• 194.85.250.154
	267A80yAhp	Get hash	malicious	Browse	• 194.85.250.154
	QJYxAALd23	Get hash	malicious	Browse	• 194.85.250.154
	z4bJfjXDDQ	Get hash	malicious	Browse	• 194.85.250.154
	XXaLHoecGp	Get hash	malicious	Browse	• 194.85.250.154
	AGiCic4uDz	Get hash	malicious	Browse	• 194.85.250.154
	3B3BMxYG8n	Get hash	malicious	Browse	• 194.85.250.154
	6WMo1OYmk3	Get hash	malicious	Browse	• 194.85.250.154
	dycuTng5W8	Get hash	malicious	Browse	• 194.85.250.154
	xINX4f5M8s	Get hash	malicious	Browse	• 194.85.250.154
	SSIuSyaBAF	Get hash	malicious	Browse	• 194.85.250.154
	IMG600094173852.exe	Get hash	malicious	Browse	• 194.85.248.115
	cdQc14SeRu	Get hash	malicious	Browse	• 194.85.248.128

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\SK TAX INV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	493568
Entropy (8bit):	7.8676652949902195
Encrypted:	false
SSDEEP:	12288:D1UFM0gixBFm0Ud7zqdz66fMPZl2t4v0f1zo0naysDDayUyhD2:D18M0gi1Kd73LD2tp3HwDRUyhD
MD5:	C2EE32F9D7DE6B05472CEDA926FD0A6F
SHA1:	D4455AC7EC0C49769B645E7471989BD7EE29F6FC
SHA-256:	84B9FEF1F2C0DD3E8F8DC93CF6574D30E2C6E5BC819599FEA60C71876DF0278D
SHA-512:	7BD853A9B3B14FEDC2CB4F14859E2A38F4AB38A6A6AAA5EA2C44BAB5D0EDF488F3BD422E8DA61DD74429E4508C09C8D0349E4995E0C8900F57E4FCD90B800 D3
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 18%, Browse • Antivirus: ReversingLabs, Detection: 20%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...dE.a.....0..~..... .....@.. ..... .@.....p...O..... ....H.....text....|.. ...~..... ..`.rsrc.....@..@.reloc..... .....@..B.....H.....e..Xv.....p.....{ ...*..{!...*..{"...*..{#...*..($....} .....}!.....}"......}#...*....0..s.....u.....f.,`(%....{ ....{ ...o&.. .,H('....{!....{!...o(...,0()....{"....{"...o*....,(+....{#....{#...o,...+..+..*..0..b..... .@d)UU.Z(%....{ ...o-...X)UU.Z('....{!...o....X)UU.Z()....{"...o/...X)UU.Z(+....{#...o0...X*...0.....r...p .....%..{ .....%q.....-.&.+.....o1....%..{!.....%q.....-.&.+.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\SK TAX INV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SK TAX INV.exe.log	
Process:	C:\Users\user\Desktop\SK TAX INV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2239
Entropy (8bit):	5.354287817410997
Encrypted:	false
SSDEEP:	48:MxHKXeHKlEHU0YHKhQnouHIW7HKjntHoxHhAHKzvr1qHXHK2HKgmHKovjHKs:iqXeqm00YqhQnouRqjntlxHeqzTw3q2W
MD5:	913D1EEA179415C6D08FB255AE42B99D
SHA1:	E994C612C0596994AAE55FBCE35B7A4FBE312FD7
SHA-256:	473B4000084ACF4C7D701CE72EBF71BD304054231B3BDF7CAF49898A1FDA13D0
SHA-512:	768045C288CEEE8FE1A099FC8CEA713B685F6ED3FD8BFA1C8E64CA09F7AF9FEBEA90F5277B28444AFF8F2AC7CD857DFCDF7D3A98CD86288925DB7A4A4234685
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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..3,"PresentationCore, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\PresentationCore\820a27781e8540ca263d835ec155f1a5\PresentationCore.ni.dll",0..3,"PresentationFramework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Presentatio5ae0f00f#\889128adc9a7c9370e5e293f65060164\PresentationFramework.ni.dll",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,"WindowsBase, Version=4.0.0.0, Culture=neutral, PublicKeyToken=31bf3856ad364e35","C:\Windows\assembly\NativeImages_v4.0.30319_32\Wi

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\SK TAX INV.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.117516745217376
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7V9NhyleajI0fuONKcpMe5i:X4LEnybgCFCtvd7V9NYRj+GONKaMv
MD5:	CF55DF705B79F961ED069D8E84D2AF1C
SHA1:	574CDF36753CF356A25872BCCAA3CC6FFCD5D23F
SHA-256:	DF982E10764D21FCB1469EB6EA1175AC69544C68900B0DD8C79A0FE8A8F300F5
SHA-512:	518A037DF1D6FBC8A296DA5B96B67E073FB1F674090AFE3243E52A65B169DE35FC041C2C05F7EEF9EC74A0100A422E53B3D7D920E5ADF6CE42B82FE94244F5DE
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...Q.F...@.h.....y.[....e..<..n....B...PP...azZ).~..Uj.>..H.b.O..AX.E.S&.O.k.3O'.Lge...$..teI....Hw.CT.].Z.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\SK TAX INV.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Moqn:Moq
MD5:	91513139ABA0F3219DD4AA39A2E0A8A1
SHA1:	F5DBA8D934ECEA79560BCF4FD578CFA1E90CD872
SHA-256:	F3708BADFB95D6F51D0611DA1DEDDD44676D73D5075C2E358F843C0AC6AA4FEB
SHA-512:	BB0CDA8E32B96AA07E5365C7AA0416F256ADA772D8C02BF70611007603895E2248034984696E6B579314B7F0EBCA8674AAB58F52B2370B4923868EB34B68AB96
Malicious:	**true**

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Reputation:	low
Preview:	^..4...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\SK TAX INV.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:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Reputation:	moderate, very likely benign file
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\SK TAX INV.exe
File Type:	data
Category:	dropped
Size (bytes):	315080
Entropy (8bit):	**7.999403263872478**
Encrypted:	**true**
SSDEEP:	6144:m8aeVE5MlgWfxwY/8uvJYRDMVpXUhXQrEBPgzC2D4Toqhs22DJM+iaPnW:mfwiMdxwYEYyWzw0TqC2kM+lnW
MD5:	981C80683A41E2D9DD9C297DAA691C54
SHA1:	7A1F5DDFFB3E630FE19E19F6AA923427DE72217B
SHA-256:	6C67B680BB9CF41F30C37D791D9EE52582977C1D9D5696FEAE1613FC0C5E2DBE
SHA-512:	72E4198AE2A65B7E1698925DF537CBA63A2877677C7C8FEA475E52B99E631272CFBEDCD5A4E1949EB7F8073C01229E89CCCD1ABBFD8832533346A6568750ADAE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	..f# ....)1*.....5....;.T..u.. .3.Xd... ....u(..._.V.{L..Y.8....~...S79.f0V...=.}...SJg|.lh.J..^Ge.....3h?n..:..r....,o."a.I....\..0Z.D.....^....[..f.I....@/_..".5+...l...J`./s..p-.....c..?...*.. .&.. ...>.Ye$=.pG.....9D...'7.w.a.[3.d.-..V..]..B.b.zA?..M..3...%A....K5@.. j.U.h.B....'...0."..u.V...d..c,r"..@9.9.>..cDgP~d9..St...{..24.s.'.....9.D..P4.....I...G..G5.....u.-2...z1[.....C..n.6.!..'.%@&.l4..P..rc+vq..C5B.b*..j.W,..T..z.....)BX4...>A.*~#..A....8..B....5....w....GC.....y.....7...?.T.....!....7A.....C.3.....A.....hC..5'..42..zS.*2.m7....A.'/.R..X....}e...>.....}...n.A...4..?.P.l..n.0.l`...".d1.(e\|..f.....i.9.#...n..+..l....Xz.q...6".Hl...+...1^pgs...%.FR.T....(...=.rHX.d.9%...?..f?.Q.yi.D9/>....V..5.....q...nP'...S.Y.....pu.!..-..\..\|/....V.....NX...../.8..V.0.5`m$.{b..lw.K.3-..C3...-.2.Qb.....o...6z....`H...(..o.ag.-7../F..RoI..O#.u|.U.@....$;.....s.~.M...j?...q#.l..y..M.[../.....=T.....5HX.QJ...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.8676652949902195
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:	SK TAX INV.exe
File size:	493568
MD5:	c2ee32f9d7de6b05472ceda926fd0a6f
SHA1:	d4455ac7ec0c49769b645e7471989bd7ee29f6fc
SHA256:	84b9fef1f2c0dd3e8f8dc93cf6574d30e2c6e5bc819599fea60c71876df0278d
SHA512:	7bd853a9b3b14fedc2cb4f14859e2a38f4ab38a6a6aaa5ea2c44bab5d0edf488f3bd422e8da61dd74429e4508c09c8d0349e4995e0c8900f57e4fcd90b8004d3

General

SSDEEP:	12288:D1UFM0gixBFm0Ud7zqdz66fMPZl2t4v0f1zo0naysDDayUyhD2:D18M0gi1Kd73LD2tp3HwDRUyhD
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...dE.a.....0..~..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x479cc2
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:	0x619F4564 [Thu Nov 25 08:12:20 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	0x77cd8	0x77e00	False	0.894757315563	data	7.87847086948	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7a000	0x5ec	0x600	False	0.438151041667	data	4.21773046757	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7c000	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
11/25/21-11:56:19.002612	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49714	8.8.8.8	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-11:56:19.127979	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	1187	192.168.2.4	194.85.248.250
11/25/21-11:56:23.493869	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58028	8.8.8.8	192.168.2.4
11/25/21-11:56:23.526666	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	1187	192.168.2.4	194.85.248.250
11/25/21-11:56:31.344296	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53097	8.8.8.8	192.168.2.4
11/25/21-11:56:31.408131	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	1187	192.168.2.4	194.85.248.250
11/25/21-11:56:37.956129	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49257	8.8.8.8	192.168.2.4
11/25/21-11:56:38.014996	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	1187	192.168.2.4	194.85.248.250
11/25/21-11:56:43.972123	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	1187	192.168.2.4	194.85.248.250
11/25/21-11:56:51.220530	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	1187	192.168.2.4	194.85.248.250
11/25/21-11:56:57.214815	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:03.772463	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49793	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:10.856473	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49821	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:17.160697	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51255	8.8.8.8	192.168.2.4
11/25/21-11:57:17.190251	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49824	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:22.257795	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52337	8.8.8.8	192.168.2.4
11/25/21-11:57:22.287984	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:29.921734	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55046	8.8.8.8	192.168.2.4
11/25/21-11:57:29.951099	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:36.010921	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49853	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:42.243149	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49285	8.8.8.8	192.168.2.4
11/25/21-11:57:42.274632	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49856	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:48.301653	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50601	8.8.8.8	192.168.2.4
11/25/21-11:57:48.330829	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49857	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:53.343018	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49859	1187	192.168.2.4	194.85.248.250
11/25/21-11:57:59.367307	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62420	8.8.8.8	192.168.2.4
11/25/21-11:57:59.485426	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49863	1187	192.168.2.4	194.85.248.250
11/25/21-11:58:06.648552	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49864	1187	192.168.2.4	194.85.248.250
11/25/21-11:58:11.655619	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49865	1187	192.168.2.4	194.85.248.250
11/25/21-11:58:17.612799	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49866	1187	192.168.2.4	194.85.248.250

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 11:56:18.956589937 CET	192.168.2.4	8.8.8.8	0xaff9	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:23.464132071 CET	192.168.2.4	8.8.8.8	0x2005	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:31.314296007 CET	192.168.2.4	8.8.8.8	0xa309	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:37.910442114 CET	192.168.2.4	8.8.8.8	0xf45d	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:43.899588108 CET	192.168.2.4	8.8.8.8	0x24c	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:51.154023886 CET	192.168.2.4	8.8.8.8	0x81cf	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:57.167371988 CET	192.168.2.4	8.8.8.8	0xbdfb	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:03.236888885 CET	192.168.2.4	8.8.8.8	0x5506	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:10.784302950 CET	192.168.2.4	8.8.8.8	0xcbd	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:17.130686998 CET	192.168.2.4	8.8.8.8	0xecb1	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:22.228977919 CET	192.168.2.4	8.8.8.8	0x62f4	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:29.875340939 CET	192.168.2.4	8.8.8.8	0x121a	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:35.943232059 CET	192.168.2.4	8.8.8.8	0xe785	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:42.213505030 CET	192.168.2.4	8.8.8.8	0x5911	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:48.256104946 CET	192.168.2.4	8.8.8.8	0x8df6	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:53.275501013 CET	192.168.2.4	8.8.8.8	0x520d	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:59.320873022 CET	192.168.2.4	8.8.8.8	0x83c	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:58:06.567533970 CET	192.168.2.4	8.8.8.8	0xc148	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:58:11.587215900 CET	192.168.2.4	8.8.8.8	0x5e4	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)
Nov 25, 2021 11:58:17.558532953 CET	192.168.2.4	8.8.8.8	0x2196	Standard query (0)	dera31.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

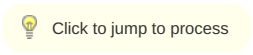
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 11:56:19.002612114 CET	8.8.8.8	192.168.2.4	0xaff9	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:23.493869066 CET	8.8.8.8	192.168.2.4	0x2005	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:31.344295979 CET	8.8.8.8	192.168.2.4	0xa309	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:37.956129074 CET	8.8.8.8	192.168.2.4	0xf45d	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:43.937406063 CET	8.8.8.8	192.168.2.4	0x24c	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:51.191472054 CET	8.8.8.8	192.168.2.4	0x81cf	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:56:57.183079004 CET	8.8.8.8	192.168.2.4	0xbdfb	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:03.274627924 CET	8.8.8.8	192.168.2.4	0x5506	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:10.822038889 CET	8.8.8.8	192.168.2.4	0xcbd	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:17.160696983 CET	8.8.8.8	192.168.2.4	0xecb1	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 11:57:22.257795095 CET	8.8.8.8	192.168.2.4	0x62f4	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:29.921734095 CET	8.8.8.8	192.168.2.4	0x121a	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:35.980635881 CET	8.8.8.8	192.168.2.4	0xe785	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:42.243149042 CET	8.8.8.8	192.168.2.4	0x5911	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:48.301652908 CET	8.8.8.8	192.168.2.4	0x8df6	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:53.313308001 CET	8.8.8.8	192.168.2.4	0x520d	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:59.367306948 CET	8.8.8.8	192.168.2.4	0x83c	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:58:06.605303049 CET	8.8.8.8	192.168.2.4	0xc148	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:58:11.625068903 CET	8.8.8.8	192.168.2.4	0x5e4	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)
Nov 25, 2021 11:58:17.579953909 CET	8.8.8.8	192.168.2.4	0x2196	No error (0)	dera31.ddns.net		194.85.248.250	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SK TAX INV.exe PID: 3980 Parent PID: 5296

General

Start time:	11:56:10
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\SK TAX INV.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SK TAX INV.exe"
Imagebase:	0x420000
File size:	493568 bytes
MD5 hash:	C2EE32F9D7DE6B05472CEDA926FD0A6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.668327294.00000000028A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.670484046.0000000003B11000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.670484046.0000000003B11000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.670484046.0000000003B11000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.668432779.0000000002965000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: SK TAX INV.exe PID: 6636 Parent PID: 3980

General

Start time:	11:56:13
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\SK TAX INV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SK TAX INV.exe
Imagebase:	0xb10000
File size:	493568 bytes
MD5 hash:	C2EE32F9D7DE6B05472CEDA926FD0A6F
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: 00000003.00000000.665221730.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.665221730.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.665221730.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.665589656.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.665589656.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.665589656.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.665941289.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.665941289.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.665941289.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.666335348.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.666335348.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.666335348.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
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: 6980 Parent PID: 3424

General

Start time:	11:56:28
Start date:	25/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x360000
File size:	493568 bytes
MD5 hash:	C2EE32F9D7DE6B05472CEDA926FD0A6F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 18%, Virustotal, Browse • Detection: 20%, ReversingLabs
Reputation:	low

Disassembly

Code Analysis