ID: 628640
Sample Name: INVOICE.exe
Cookbook: default.jbs
Time: 20:28:39
Date: 17/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

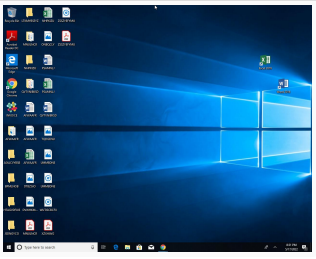
Windows Analysis Report

INVOICE.exe

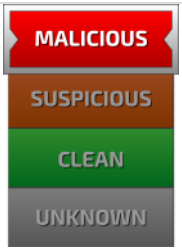
Overview

General Information

Sample Name:	INVOICE.exe
Analysis ID:	628640
MD5:	9d58123708f80d..
SHA1:	27317b8dbf3474..
SHA256:	b9066fabc29448..
Tags:	exe NanoCore
Infos:	



Detection



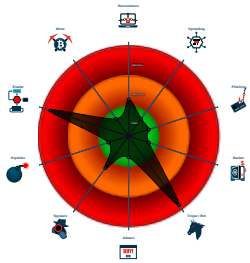
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Initial sample is a PE file and has a…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- INVOICE.exe (PID: 3004 cmdline: "C:\Users\user\Desktop\INVOICE.exe" MD5: 9D58123708F80D79654D981A8B6D9924)
  - INVOICE.exe (PID: 3488 cmdline: C:\Users\user\Desktop\INVOICE.exe MD5: 9D58123708F80D79654D981A8B6D9924)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "fe56abb4-cb76-44f1-89b4-7bb11730",
  "Group": "Default",
  "Domain1": "deranano2.ddns.net",
  "Port": 1187,
  "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 Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.489522906.0000000002B4E000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000003.00000000.480652507.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000003.00000000.480652507.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000003.00000000.480652507.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000000.00000002.495513796.0000000007300000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_zgRAT	Detects zgRAT	ditekSHen	• 0x51d2f:$s1: file:/// • 0x51c3f:$s2: {11111-22222-10009-11112} • 0x51cbf:$s3: {11111-22222-50001-00000} • 0x4f0a5:$s4: get_Module • 0x4f4eb:$s5: Reverse • 0x5156e:$s6: BlockCopy • 0x513b2:$s7: ReadByte • 0x51d41:$s8: 4C 00 6F 00 63 00 61 00 74 00 69 00 6F 00 6E 00 00 0B 46 00 69 00 6E 00 64 00 20 00 00 13 52 00 65 00 73 00 6F 00 75 00 72 00 63 00 65 00 41 00 00 11 56 00 69 00 72 00 74 00 75 00 61 00 6C 00 ...

Click to see the 20 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.INVOICE.exe.400000.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
3.0.INVOICE.exe.400000.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$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.INVOICE.exe.400000.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.0.INVOICE.exe.400000.4.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xfef5:$x1: NanoCore Client • 0xff05:$x1: NanoCore Client • 0x1014d:$x2: NanoCore.ClientPlugin • 0x1018d:$x3: NanoCore.ClientPluginHost • 0x10142:$i1: IClientApp • 0x10163:$i2: IClientData • 0x1016f:$i3: IClientNetwork • 0x1017e:$i4: IClientAppHost • 0x101a7:$i5: IClientDataHost • 0x101b7:$i6: IClientLoggingHost • 0x101ca:$i7: IClientNetworkHost • 0x101dd:$i8: IClientUIHost • 0x101eb:$i9: IClientNameObjectCollection • 0x10207:$i10: IClientReadOnlyNameObjectCollection • 0xff54:$s1: ClientPlugin • 0x10156:$s1: ClientPlugin • 0x1064a:$s2: EndPoint • 0x10653:$s3: IPAddress • 0x1065d:$s4: IPEndPoint • 0x12093:$s6: get_ClientSettings • 0x12637:$s7: get_Connected
3.0.INVOICE.exe.400000.4.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$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

Click to see the 47 entries

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044981511872816766 05/17/22-20:31:37.145576
SID:	2816766
Source Port:	49815
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044979411872816766 05/17/22-20:30:47.656373
SID:	2816766
Source Port:	49794
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 212.193.30.204 - Destination IP: 192.168.2.5	
Timestamp:	212.193.30.204192.168.2.51187498182841753 05/17/22-20:31:48.726428
SID:	2841753
Source Port:	1187
Destination Port:	49818
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 212.193.30.204 - Destination IP: 192.168.2.5	
Timestamp:	212.193.30.204192.168.2.51187498192841753 05/17/22-20:31:53.756641
SID:	2841753
Source Port:	1187
Destination Port:	49819
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044982211872816766 05/17/22-20:31:58.715420
SID:	2816766
Source Port:	49822
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044980611872816766 05/17/22-20:31:10.821016
SID:	2816766
Source Port:	49806
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044980311872025019 05/17/22-20:31:00.853122
SID:	2025019
Source Port:	49803
Destination Port:	1187

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044979711872025019 05/17/22-20:30:54.580308
SID:	2025019
Source Port:	49797
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044980311872816718 05/17/22-20:31:01.197924
SID:	2816718
Source Port:	49803
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044978711872816766 05/17/22-20:30:40.618852
SID:	2816766
Source Port:	49787
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 212.193.30.204 - Destination IP: 192.168.2.5	
Timestamp:	212.193.30.204192.168.2.51187498222841753 05/17/22-20:32:03.661713
SID:	2841753
Source Port:	1187
Destination Port:	49822
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044979711872816766 05/17/22-20:30:55.725499
SID:	2816766
Source Port:	49797
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044978711872025019 05/17/22-20:30:38.957783
SID:	2025019
Source Port:	49787
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044981611872025019 05/17/22-20:31:42.303773
SID:	2025019
Source Port:	49816
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 212.193.30.204 - Destination IP: 192.168.2.5

Timestamp:	212.193.30.204192.168.2.51187498122841753 05/17/22-20:31:22.376109
SID:	2841753
Source Port:	1187
Destination Port:	49812
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204

Timestamp:	192.168.2.5212.193.30.2044980611872025019 05/17/22-20:31:07.938867
SID:	2025019
Source Port:	49806
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204

Timestamp:	192.168.2.5212.193.30.2044980911872816766 05/17/22-20:31:17.197289
SID:	2816766
Source Port:	49809
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204

Timestamp:	192.168.2.5212.193.30.2044978111872025019 05/17/22-20:30:31.001024
SID:	2025019
Source Port:	49781
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204

Timestamp:	192.168.2.5212.193.30.2044980911872025019 05/17/22-20:31:15.942780
SID:	2025019
Source Port:	49809
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204

Timestamp:	192.168.2.5212.193.30.2044981211872025019 05/17/22-20:31:22.345784
SID:	2025019
Source Port:	49812
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204

Timestamp:	192.168.2.5212.193.30.2044981911872025019 05/17/22-20:31:53.726213
SID:	2025019
Source Port:	49819
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204

Timestamp:	192.168.2.5212.193.30.2044982211872025019 05/17/22-20:31:58.625380
SID:	2025019
Source Port:	49822
Destination Port:	1187

Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044979411872025019 05/17/22-20:30:46.018194
SID:	2025019
Source Port:	49794
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044981511872025019 05/17/22-20:31:36.233314
SID:	2025019
Source Port:	49815
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044981611872816766 05/17/22-20:31:43.265162
SID:	2816766
Source Port:	49816
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044977211872816766 05/17/22-20:30:24.595254
SID:	2816766
Source Port:	49772
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044981311872025019 05/17/22-20:31:29.263030
SID:	2025019
Source Port:	49813
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044981811872025019 05/17/22-20:31:48.698744
SID:	2025019
Source Port:	49818
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	
Timestamp:	192.168.2.5212.193.30.2044981311872816766 05/17/22-20:31:31.058415
SID:	2816766
Source Port:	49813
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204

Timestamp:	192.168.2.5212.193.30.2044977211872025019 05/17/22-20:30:22.925084
SID:	2025019
Source Port:	49772
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	−
Timestamp:	192.168.2.5212.193.30.2044978111872816766 05/17/22-20:30:33.613252
SID:	2816766
Source Port:	49781
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 212.193.30.204 - Destination IP: 192.168.2.5	−
Timestamp:	212.193.30.204192.168.2.51187497942810290 05/17/22-20:30:47.256191
SID:	2810290
Source Port:	1187
Destination Port:	49794
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.5 - Destination IP: 212.193.30.204	−
Timestamp:	192.168.2.5212.193.30.2044980311872816766 05/17/22-20:31:02.293623
SID:	2816766
Source Port:	49803
Destination Port:	1187
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic
- 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

.NET source code contains method to dynamically call methods (often used by packers)

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

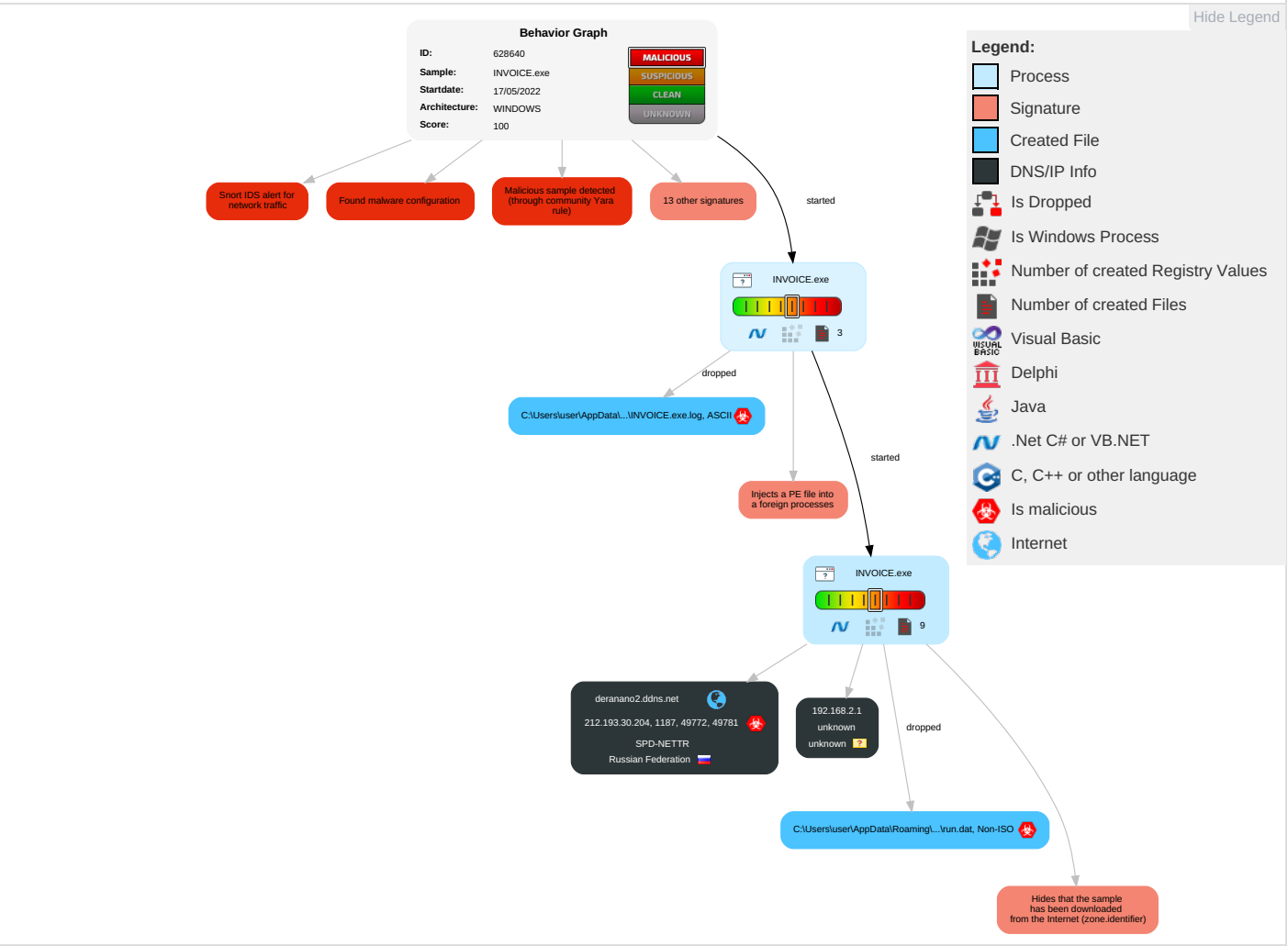
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	1 Input Capture	1 Query Registry	Remote Services	1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	1 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 1 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	2 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 2 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 Obfuscated Files or Information	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

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
INVOICE.exe	27%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
INVOICE.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Source	Detection	Scanner	Label	Link	Download
3.0.INVOICE.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
deranano2.ddns.net	100%	Avira URL Cloud	malware	
http://www.fontbureau.comdiao2	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
deranano2.ddns.net	212.193.30.204	true	true		unknown

Contacted URLs

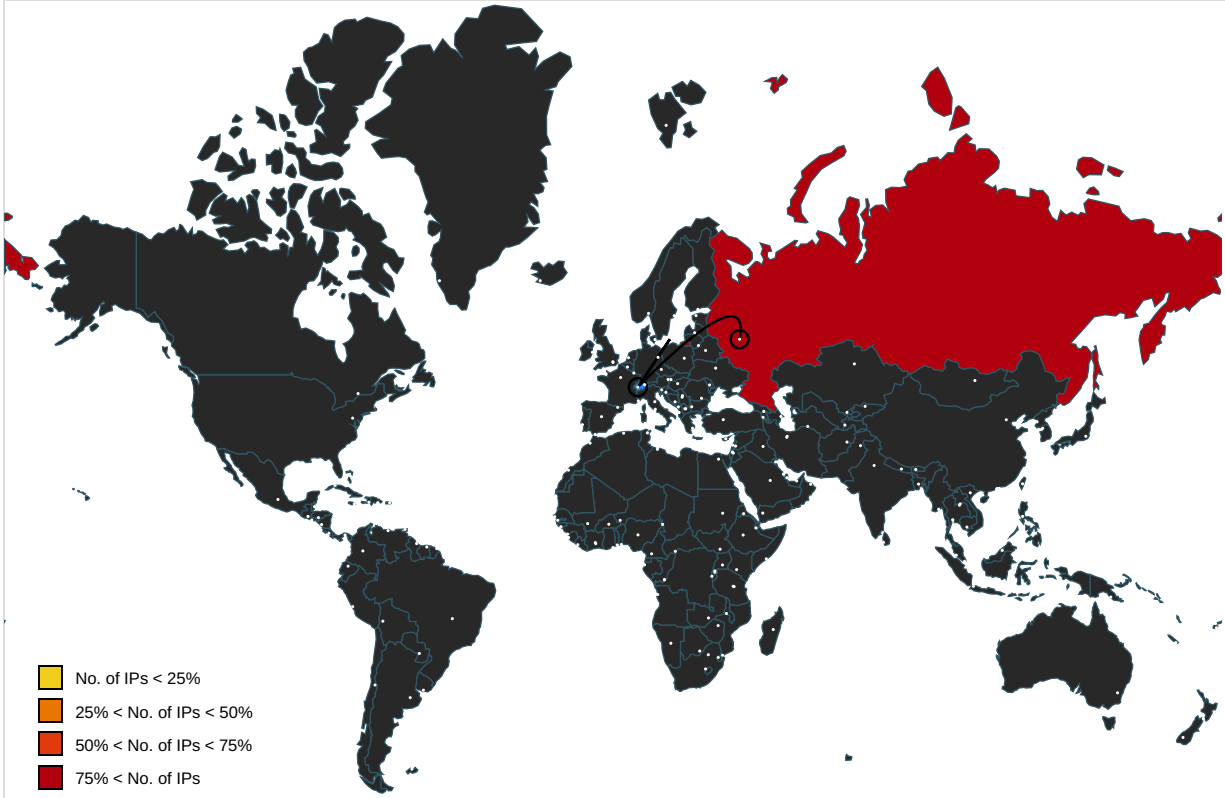
Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
deranano2.ddns.net	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma	INVOICE.exe, 00000000.00000002.484971382.00000000005C7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comiona	INVOICE.exe, 00000000.00000002.484971382.00000000005C7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comdiao2	INVOICE.exe, 00000000.00000002.484971382.00000000005C7000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	INVOICE.exe, 00000000.00000002.493957274.0000000006912000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
212.193.30.204	deranano2.ddns.net	Russian Federation		57844	SPD-NETTR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	628640
Start date and time: 17/05/202220:28:39	2022-05-17 20:28:39 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	INVOICE.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
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@3/5@15/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 42.3% • Quality standard deviation: 32.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 20.223.24.244
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, neu-displaycatalogrp.frontdoor.bigcatalog.commerce.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, consumer-displaycatalogrp-aks2aks-europe.md.mp.microsoft.com.akadns.net, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- VT rate limit hit for: INVOICE.exe

Simulations

Behavior and APIs

Time	Type	Description
20:30:06	API Interceptor	795x Sleep call for process: INVOICE.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\INVOICE.exe

File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4FsXE8:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHJ
MD5:	EA78C102145ED608EF0E407B978AF339
SHA1:	66C9179ED9675B9271A97AB1FC878077E09AB731
SHA-256:	8BF01E0C445BD07C0B4EDC7199B7E17DAF1CA55CA52D4A6EAC4EF211C2B1A73E
SHA-512:	8C04139A1FC3C3BDACB680EC443615A43EB18E73B5A0CFCA644CB4A5E71746B275B3E238DD1A5A205405313E457BB75F9BBB93277C67AFA5D78DCFA30E5DA02B
Malicious:	**true**
Reputation:	moderate, 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..2,"Microsoft.VisualBasic, Version=10.0.0.0, 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\INVOICE.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
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.....&.

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

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:q8l9tn:q8Fn
MD5:	A8BADF4E8D986108589909B1AE02C207
SHA1:	80D375744D4B880EE40956B61AB5E7E3B6C696FE
SHA-256:	B9FE1CD4CAEDEADEAE92F8C70EDA0B0DA99FDCC0DC788157D7B28AE6799AA06F
SHA-512:	5F1C1FB140D9BA7FF5FD373742A116237C8665ED483FE4950D41F5AB729711162223CAF840879E52E03B51949DB7608039C839EE77FD0A8DD10C2723F0406336
Malicious:	**true**
Reputation:	low
Preview:	E.Y.~8.H

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

Process:	C:\Users\user\Desktop\INVOICE.exe
File Type:	data
Category:	dropped
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\INVOICE.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E926
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..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV.,.,..0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&.jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_..&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..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):	7.935606119244415
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:	INVOICE.exe
File size:	656896
MD5:	9d58123708f80d79654d981a8b6d9924
SHA1:	27317b8dbf347408865b071cd40f8c97d1522482
SHA256:	b9066fabc2944828b98d6f22985038c59a5f6cfb1ae09b2f6b5c89bf87a43c44
SHA512:	f6b5cfbe894549644337e605513e3d8d517c16a167141eb693033d95ff5c9b95f6a8a72090605dd9817827a5453abc828d7a1ec4088afe019151cbddeed8a2b8
SSDEEP:	12288:nsWyvNVQClWSEqOPhn/qu09/c3OwKjGes84ChuNtrzMnrj3NcMs0Tve:nsWI7WSEv/ql/mOjZsiuN5z6sQ
TLSH:	29D4120A709EEB3BC97CB7F95441525013B1B22B3457E32C9ECAE0C75A9BF406685B17
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...og.b.....0.....@.....V.... .....@.. .....`.....@.....

File Icon

Icon Hash:	64e4d2eeacd6d819

Static PE Info

General

Entrypoint:	0x49e356
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:	0x6283676F [Tue May 17 09:14:23 2022 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

Instruction
jmp dword ptr [00402000h]
add dword ptr [eax], eax
add byte ptr [eax], al
add al, byte ptr [eax]
add byte ptr [eax], al
add eax, dword ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
pop ds
add byte ptr [eax], al
add bh, bh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9e304	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa0000	0x3c74	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x9e1cc	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x9c39c	0x9c400	False	0.9418953125	data	7.94289795658	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa0000	0x3c74	0x3e00	False	0.92244203629	data	7.6910187968	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xa4000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xa00c8	0x3832	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xa390c	0x14	data		
RT_VERSION	0xa3930	0x340	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Chandler's 2022 (C)
Assembly Version	1.1.0.0
InternalName	IObjectRefere.exe
FileVersion	1.1.0.0
CompanyName	Chandler's
LegalTrademarks	
Comments	
ProductName	TemporalToolkit
ProductVersion	1.1.0.0
FileDescription	
OriginalFilename	IObjectRefere.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5212.193.30.2044981511872816766 05/17/22-20:31:37.145576	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49815	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.2044979411872816766 05/17/22-20:30:47.656373	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49794	1187	192.168.2.5	212.193.30.204
212.193.30.204192.168.2.51187498182841753 05/17/22-20:31:48.726428	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1187	49818	212.193.30.204	192.168.2.5
212.193.30.204192.168.2.51187498192841753 05/17/22-20:31:53.756641	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1187	49819	212.193.30.204	192.168.2.5
192.168.2.5212.193.30.2044982211872816766 05/17/22-20:31:58.715420	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49822	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.2044980611872816766 05/17/22-20:31:10.821016	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49806	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.2044980311872025019 05/17/22-20:31:00.853122	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49803	1187	192.168.2.5	212.193.30.204

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5212.193.30.20 44979711872025019 05/17/22-20:30:54.580308	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44980311872816718 05/17/22-20:31:01.197924	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49803	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44978711872816766 05/17/22-20:30:40.618852	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49787	1187	192.168.2.5	212.193.30.204
212.193.30.204192.168.2.5118749822284175 3 05/17/22-20:32:03.661713	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1187	49822	212.193.30.204	192.168.2.5
192.168.2.5212.193.30.20 44979711872816766 05/17/22-20:30:55.725499	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49797	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44978711872025019 05/17/22-20:30:38.957783	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44981611872025019 05/17/22-20:31:42.303773	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	1187	192.168.2.5	212.193.30.204
212.193.30.204192.168.2.5118749812284175 3 05/17/22-20:31:22.376109	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	1187	49812	212.193.30.204	192.168.2.5
192.168.2.5212.193.30.20 44980611872025019 05/17/22-20:31:07.938867	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49806	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44980911872816766 05/17/22-20:31:17.197289	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49809	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44978111872025019 05/17/22-20:30:31.001024	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44980911872025019 05/17/22-20:31:15.942780	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49809	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44981211872025019 05/17/22-20:31:22.345784	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49812	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44981911872025019 05/17/22-20:31:53.726213	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44982211872025019 05/17/22-20:31:58.625380	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49822	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44979411872025019 05/17/22-20:30:46.018194	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49794	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44981511872025019 05/17/22-20:31:36.233314	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44981611872816766 05/17/22-20:31:43.265162	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49816	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.20 44977211872816766 05/17/22-20:30:24.595254	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49772	1187	192.168.2.5	212.193.30.204

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5212.193.30.204498131187202501905/17/22-20:31:29.263030	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.204498181187202501905/17/22-20:31:48.698744	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49818	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.204498131187281676605/17/22-20:31:31.058415	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49813	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.204497721187202501905/17/22-20:30:22.925084	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	1187	192.168.2.5	212.193.30.204
192.168.2.5212.193.30.204497811187281676605/17/22-20:30:33.613252	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49781	1187	192.168.2.5	212.193.30.204
212.193.30.204192.168.2.51187497942810290 05/17/22-20:30:47.256191	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	1187	49794	212.193.30.204	192.168.2.5
192.168.2.5212.193.30.204498031187281676605/17/22-20:31:02.293623	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49803	1187	192.168.2.5	212.193.30.204

Network Port Distribution

Total Packets: 39

- 53 (DNS)
- 1187 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2022 20:30:22.785531044 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:22.812949896 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:22.813136101 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:22.925084114 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:22.968403101 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:22.978699923 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.006140947 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.148186922 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.257045984 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.332336903 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.373541117 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.373573065 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.373589993 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.373610973 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.373697042 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.400897980 CEST	1187	49772	212.193.30.204	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2022 20:30:23.400927067 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.400942087 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.400959015 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.400975943 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.400989056 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.400991917 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.401010990 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.401016951 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.401030064 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.401040077 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.401334047 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.427997112 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428025007 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428041935 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428057909 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428075075 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428091049 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428100109 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.428107977 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428128004 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428144932 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428148985 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.428163052 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428167105 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.428180933 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428198099 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428214073 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.428215027 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428234100 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428236008 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.428251982 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428272009 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.428286076 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.428317070 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.455166101 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455198050 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455214977 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455231905 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455249071 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455265045 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455281973 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455298901 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455317020 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455332994 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455348969 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455365896 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455383062 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455399036 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455415964 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455431938 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455450058 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455467939 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455485106 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455502033 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455518961 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455534935 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455550909 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455566883 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455584049 CEST	1187	49772	212.193.30.204	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2022 20:30:23.455601931 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455617905 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455634117 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455650091 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455666065 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455682039 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455698967 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.455773115 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.455830097 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.483926058 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.483972073 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484000921 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484030008 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484041929 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.484057903 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484086990 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484095097 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.484117031 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484143019 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484144926 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.484170914 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484198093 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484224081 CEST	49772	1187	192.168.2.5	212.193.30.204
May 17, 2022 20:30:23.484225988 CEST	1187	49772	212.193.30.204	192.168.2.5
May 17, 2022 20:30:23.484257936 CEST	1187	49772	212.193.30.204	192.168.2.5

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 17, 2022 20:30:22.744570971 CEST	54322	53	192.168.2.5	8.8.8.8
May 17, 2022 20:30:22.764415979 CEST	53	54322	8.8.8.8	192.168.2.5
May 17, 2022 20:30:30.888555050 CEST	63187	53	192.168.2.5	8.8.8.8
May 17, 2022 20:30:30.910044909 CEST	53	63187	8.8.8.8	192.168.2.5
May 17, 2022 20:30:38.901221037 CEST	61941	53	192.168.2.5	8.8.8.8
May 17, 2022 20:30:38.922380924 CEST	53	61941	8.8.8.8	192.168.2.5
May 17, 2022 20:30:45.969238997 CEST	63241	53	192.168.2.5	8.8.8.8
May 17, 2022 20:30:45.988259077 CEST	53	63241	8.8.8.8	192.168.2.5
May 17, 2022 20:30:54.377773046 CEST	57809	53	192.168.2.5	8.8.8.8
May 17, 2022 20:30:54.399000883 CEST	53	57809	8.8.8.8	192.168.2.5
May 17, 2022 20:31:00.802875042 CEST	62680	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:00.823893070 CEST	53	62680	8.8.8.8	192.168.2.5
May 17, 2022 20:31:07.682859898 CEST	49912	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:07.700628042 CEST	53	49912	8.8.8.8	192.168.2.5
May 17, 2022 20:31:15.894793987 CEST	57990	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:15.914181948 CEST	53	57990	8.8.8.8	192.168.2.5
May 17, 2022 20:31:22.294926882 CEST	54463	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:22.315357924 CEST	53	54463	8.8.8.8	192.168.2.5
May 17, 2022 20:31:29.212796926 CEST	63718	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:29.232027054 CEST	53	63718	8.8.8.8	192.168.2.5
May 17, 2022 20:31:36.179580927 CEST	61126	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:36.196830034 CEST	53	61126	8.8.8.8	192.168.2.5
May 17, 2022 20:31:42.240658998 CEST	54152	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:42.261655092 CEST	53	54152	8.8.8.8	192.168.2.5
May 17, 2022 20:31:48.642363071 CEST	53194	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:48.660270929 CEST	53	53194	8.8.8.8	192.168.2.5
May 17, 2022 20:31:53.676034927 CEST	50393	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:53.695802927 CEST	53	50393	8.8.8.8	192.168.2.5
May 17, 2022 20:31:58.573787928 CEST	61458	53	192.168.2.5	8.8.8.8
May 17, 2022 20:31:58.593518019 CEST	53	61458	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 17, 2022 20:30:22.744570971 CEST	192.168.2.5	8.8.8.8	0x262e	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:30:30.888555050 CEST	192.168.2.5	8.8.8.8	0xff17	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:30:38.901221037 CEST	192.168.2.5	8.8.8.8	0x2997	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:30:45.969238997 CEST	192.168.2.5	8.8.8.8	0xb8ef	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:30:54.377773046 CEST	192.168.2.5	8.8.8.8	0x40dd	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:00.802875042 CEST	192.168.2.5	8.8.8.8	0xd7d7	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:07.682859898 CEST	192.168.2.5	8.8.8.8	0xb849	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:15.894793987 CEST	192.168.2.5	8.8.8.8	0x9ea0	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:22.294926882 CEST	192.168.2.5	8.8.8.8	0xf974	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:29.212796926 CEST	192.168.2.5	8.8.8.8	0xf8e0	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:36.179580927 CEST	192.168.2.5	8.8.8.8	0xd91b	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:42.240658998 CEST	192.168.2.5	8.8.8.8	0xf075	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:48.642363071 CEST	192.168.2.5	8.8.8.8	0x4878	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:53.676034927 CEST	192.168.2.5	8.8.8.8	0xa5d3	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)
May 17, 2022 20:31:58.573787928 CEST	192.168.2.5	8.8.8.8	0xe914	Standard query (0)	deranano2.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 17, 2022 20:30:22.764415979 CEST	8.8.8.8	192.168.2.5	0x262e	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:30:30.910044909 CEST	8.8.8.8	192.168.2.5	0xff17	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:30:38.922380924 CEST	8.8.8.8	192.168.2.5	0x2997	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:30:45.988259077 CEST	8.8.8.8	192.168.2.5	0xb8ef	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:30:54.399000883 CEST	8.8.8.8	192.168.2.5	0x40dd	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:00.823893070 CEST	8.8.8.8	192.168.2.5	0xd7d7	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:07.700628042 CEST	8.8.8.8	192.168.2.5	0xb849	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:15.914181948 CEST	8.8.8.8	192.168.2.5	0x9ea0	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:22.315357924 CEST	8.8.8.8	192.168.2.5	0xf974	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:29.232027054 CEST	8.8.8.8	192.168.2.5	0xf8e0	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:36.196830034 CEST	8.8.8.8	192.168.2.5	0xd91b	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:42.261655092 CEST	8.8.8.8	192.168.2.5	0xf075	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:48.660270929 CEST	8.8.8.8	192.168.2.5	0x4878	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:53.695802927 CEST	8.8.8.8	192.168.2.5	0xa5d3	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)
May 17, 2022 20:31:58.593518019 CEST	8.8.8.8	192.168.2.5	0xe914	No error (0)	deranano2.ddns.net		212.193.30.204	A (IP address)	IN (0x0001)

Statistics

Behavior

System Behavior

Analysis Process: INVOICE.exe PID: 3004, Parent PID: 384

General

Target ID:	0
Start time:	20:29:53
Start date:	17/05/2022
Path:	C:\Users\user\Desktop\INVOICE.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\INVOICE.exe"
Imagebase:	0x3d0000
File size:	656896 bytes
MD5 hash:	9D58123708F80D79654D981A8B6D9924
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: 00000000.00000002.489522906.0000000002B4E000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.495513796.0000000007300000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.487374946.0000000002851000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.489936626.00000000039CB000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.489936626.00000000039CB000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.489936626.00000000039CB000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E3FCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E3FCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INVOICE.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E70C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\INVOICE.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E70C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D341B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D341B4F	ReadFile

Analysis Process: INVOICE.exe PID: **3488**, Parent PID: **3004**

General

Target ID:	3
Start time:	20:30:14
Start date:	17/05/2022

Path:	C:\Users\user\Desktop\INVOICE.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\INVOICE.exe
Imagebase:	0xb40000
File size:	656896 bytes
MD5 hash:	9D58123708F80D79654D981A8B6D9924
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: 00000003.00000000.480652507.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.480652507.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.480652507.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.482727017.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.482727017.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.482727017.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.481241777.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.481241777.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.481241777.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000000.481993542.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000000.481993542.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000000.481993542.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E3FCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E3FCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D34BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D341E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D34BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D34BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	14	6D341E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D341E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D341E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\INVOICE.exe:Zone.Identifier	success or wait	1	6D2C2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	45 fd 59 fd 7e 38 fd 48	EY~8H	success or wait	1	6D341B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	10	6D341B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	6D341B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6D341B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D341B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D341B4F	ReadFile
C:\Users\user\Desktop\INVOICE.exe	unknown	4096	success or wait	1	6E3BD72F	unknown
C:\Users\user\Desktop\INVOICE.exe	unknown	512	success or wait	1	6E3BD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6E3BD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6E3BD72F	unknown

Disassembly

No disassembly