ID: 709347
Sample Name:
SdwkQEBnc3.exe
Cookbook: default.jbs
Time: 10:37:05
Date: 25/09/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

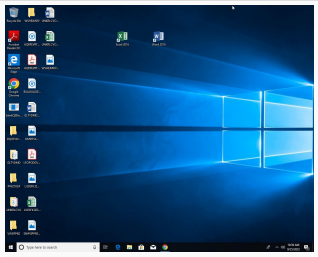
Windows Analysis Report

SdwkQEBnc3.exe

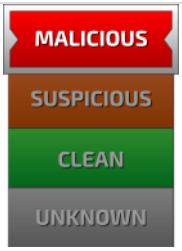
Overview

General Information

Sample Name:	SdwkQEBnc3.exe
Analysis ID:	709347
MD5:	33851c19216f0e..
SHA1:	0ad881c7d507be..
SHA256:	d3c3718f2106ac…
Tags:	exe NanoCore RAT
Infos:	YARA SIGMA



Detection



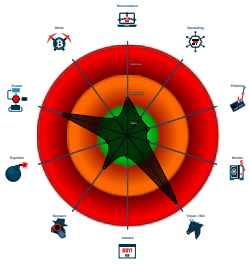
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Machine Learning detection for sam…
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- SdwkQEBnc3.exe (PID: 5128 cmdline: "C:\Users\user\Desktop\SdwkQEBnc3.exe" MD5: 33851C19216F0E65DB0AECC27DC71FFC)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7fd0fb12-397b-455a-940b-bef9261b",
  "Group": "kurban",
  "Domain1": "eu-central-7075.packetriot.net",
  "Domain2": "127.0.0.1",
  "Port": 22378,
  "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

Initial Sample

Source	Rule	Description	Author	Strings
SdwkQEBnc3.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
SdwkQEBnc3.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
SdwkQEBnc3.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
SdwkQEBnc3.exe	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

Source	Rule	Description	Author	Strings
SdwkQEBnc3.exe	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 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.239926624.0000000000F12000.00000002.00000001.01000000.00000003.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000000.239926624.0000000000F12000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000000.239926624.0000000000F12000.00000002.00000001.01000000.00000003.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000000.00000000.239926624.0000000000F12000.00000002.00000001.01000000.00000003.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xff8d:$a1: NanoCore.ClientPluginHost • 0xff4d:$a2: NanoCore.ClientPlugin • 0x11ea6:$b1: get_BuilderSettings • 0xfda9:$b2: ClientLoaderForm.resources • 0x115c6:$b3: PluginCommand • 0xff7e:$b4: IClientAppHost • 0x1a3fe:$b5: GetBlockHash • 0x124fe:$b6: AddHostEntry • 0x161f1:$b7: LogClientException • 0x1246b:$b8: PipeExists • 0xffb7:$b9: IClientLoggingHost
00000000.00000002.511555903.0000000004637000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 16 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SdwkQEBnc3.exe.463e424.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
0.2.SdwkQEBnc3.exe.463e424.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
0.2.SdwkQEBnc3.exe.463e424.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
0.2.SdwkQEBnc3.exe.463e424.3.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xd978:$x2: NanoCore.ClientPlugin • 0xd9ad:$x3: NanoCore.ClientPluginHost • 0xd96c:$i2: IClientData • 0xd98e:$i3: IClientNetwork • 0xd99d:$i5: IClientDataHost • 0xd9c7:$i6: IClientLoggingHost • 0xd9da:$i7: IClientNetworkHost • 0xd9ed:$i8: IClientUIHost • 0xd9fb:$i9: IClientNameObjectCollection • 0xda17:$i10: IClientReadOnlyNameObjectCollection • 0xd76a:$s1: ClientPlugin • 0xd981:$s1: ClientPlugin • 0x129a2:$s6: get_ClientSettings
0.2.SdwkQEBnc3.exe.463e424.3.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xd9ad:$a1: NanoCore.ClientPluginHost • 0xd978:$a2: NanoCore.ClientPlugin • 0x128f3:$b1: get_BuilderSettings • 0x12862:$b7: LogClientException • 0xd9c7:$b9: IClientLoggingHost
Click to see the 45 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116 −

Timestamp:	192.168.2.3167.71.56.11649729223782025019 09/25/22-10:39:19.021240
SID:	2025019
Source Port:	49729
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116 −

Timestamp:	192.168.2.3167.71.56.11649708223782025019 09/25/22-10:37:58.335400
SID:	2025019
Source Port:	49708
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116 −

Timestamp:	192.168.2.3167.71.56.11649719223782025019 09/25/22-10:38:45.572488
SID:	2025019

Source Port:	49719
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649728223782025019 09/25/22-10:39:13.005416
SID:	2025019
Source Port:	49728
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649723223782025019 09/25/22-10:39:06.622577
SID:	2025019
Source Port:	49723
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649709223782025019 09/25/22-10:38:04.391752
SID:	2025019
Source Port:	49709
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649712223782025019 09/25/22-10:38:11.114012
SID:	2025019
Source Port:	49712
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649723223782816766 09/25/22-10:39:08.421800
SID:	2816766
Source Port:	49723
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649733223782816766 09/25/22-10:39:42.564776
SID:	2816766
Source Port:	49733
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649712223782816766 09/25/22-10:38:14.198704
SID:	2816766
Source Port:	49712
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.11649737223782025019 09/25/22-10:39:46.930085
SID:	2025019
Source Port:	49737
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.11649716223782025019 09/25/22-10:38:33.571963
SID:	2025019
Source Port:	49716
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.11649717223782025019 09/25/22-10:38:39.534899
SID:	2025019
Source Port:	49717
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.11649708223782816718 09/25/22-10:37:59.384612
SID:	2816718
Source Port:	49708
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.11649716223782816766 09/25/22-10:38:35.293304
SID:	2816766
Source Port:	49716
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.11649737223782816766 09/25/22-10:39:48.190268
SID:	2816766
Source Port:	49737
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.11649729223782816766 09/25/22-10:39:20.875554
SID:	2816766
Source Port:	49729
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.11649719223782816766 09/25/22-10:38:47.309965
SID:	2816766
Source Port:	49719

Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649708223782816766 09/25/22-10:38:00.056144
SID:	2816766
Source Port:	49708
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649717223782816766 09/25/22-10:38:41.356311
SID:	2816766
Source Port:	49717
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649728223782816766 09/25/22-10:39:14.776089
SID:	2816766
Source Port:	49728
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649741223782816766 09/25/22-10:39:54.862352
SID:	2816766
Source Port:	49741
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649723223782816718 09/25/22-10:39:07.608396
SID:	2816718
Source Port:	49723
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649733223782025019 09/25/22-10:39:40.736255
SID:	2025019
Source Port:	49733
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	−
Timestamp:	192.168.2.3167.71.56.11649709223782816766 09/25/22-10:38:06.120867
SID:	2816766
Source Port:	49709
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 167.71.56.116	
Timestamp:	192.168.2.3167.71.56.1164974122378202501 9 09/25/22-10:39:53.012867
SID:	2025019
Source Port:	49741
Destination Port:	22378
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

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)

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

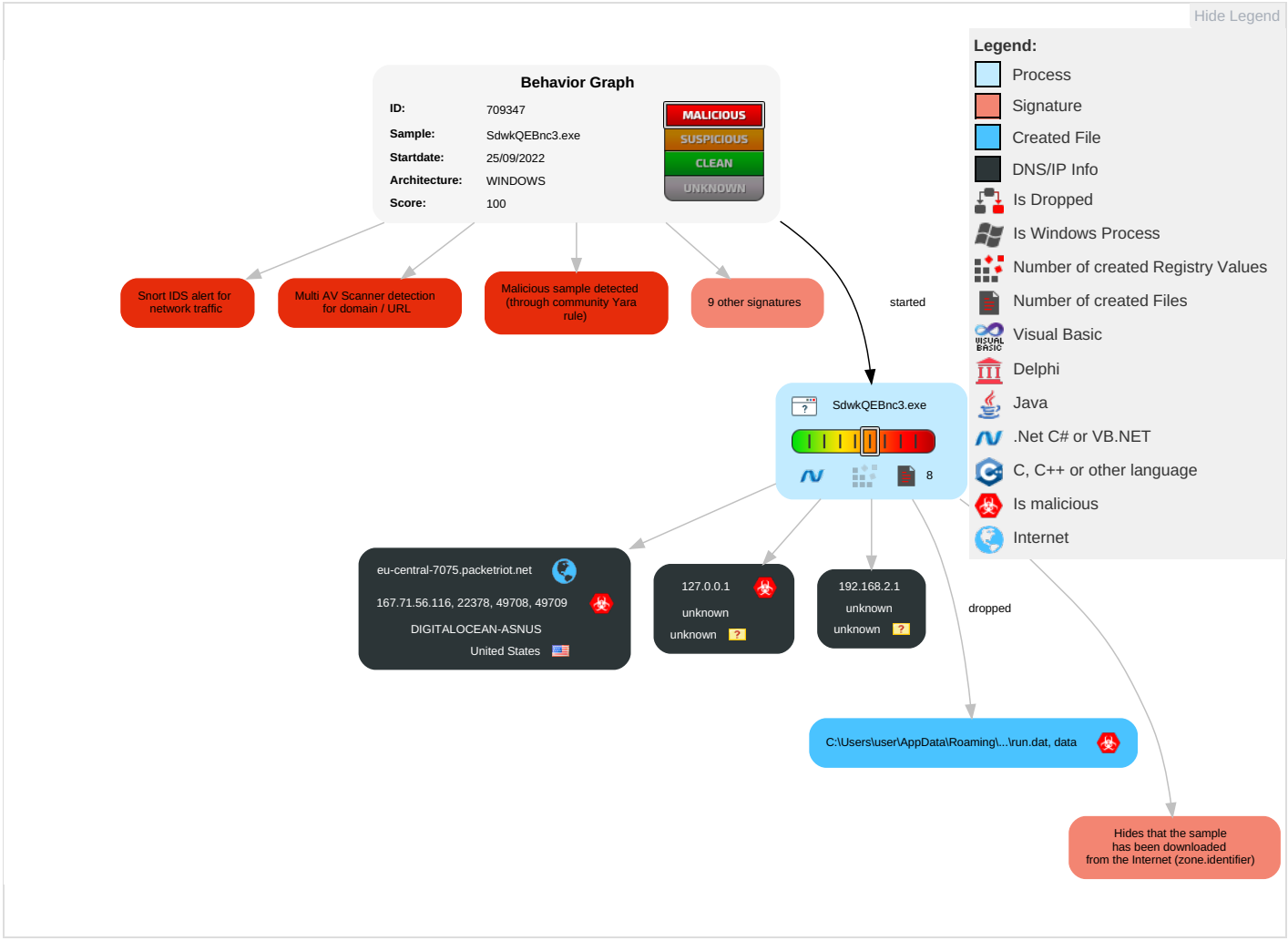
Detected Nanocore Rat

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	Windows Management Instrumentation	Path Interception	1 Access Token Manipulation	1 Masquerading	2 1 Input Capture	1 Security Software Discovery	Remote Services	2 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	1 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 Process 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	2 1 Virtualization/Sandbox Evasion	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 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Process Injection	LSA Secrets	3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	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
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 2 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

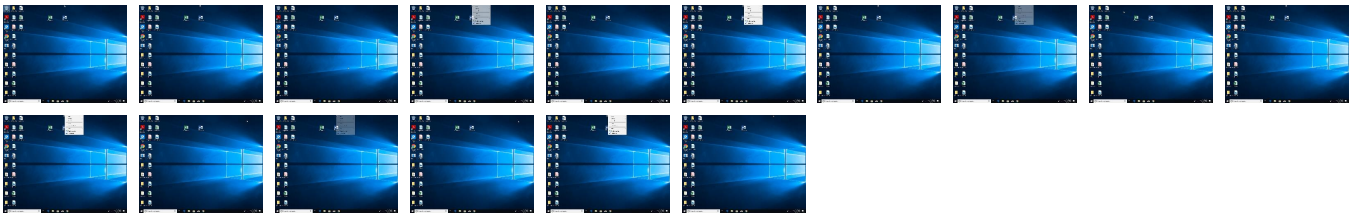
Behavior Graph



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
SdwkQEBnc3.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
SdwkQEBnc3.exe	83%	Virustotal		Browse
SdwkQEBnc3.exe	94%	Metadefender		Browse
SdwkQEBnc3.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
SdwkQEBnc3.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.SdwkQEBnc3.exe.f10000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.SdwkQEBnc3.exe.5e30000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
eu-central-7075.packetriot.net	10%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
eu-central-7075.packetriot.net	10%	Virustotal		Browse
127.0.0.1	1%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	
eu-central-7075.packetriot.net	100%	Avira URL Cloud	malware	

Domains and IPs

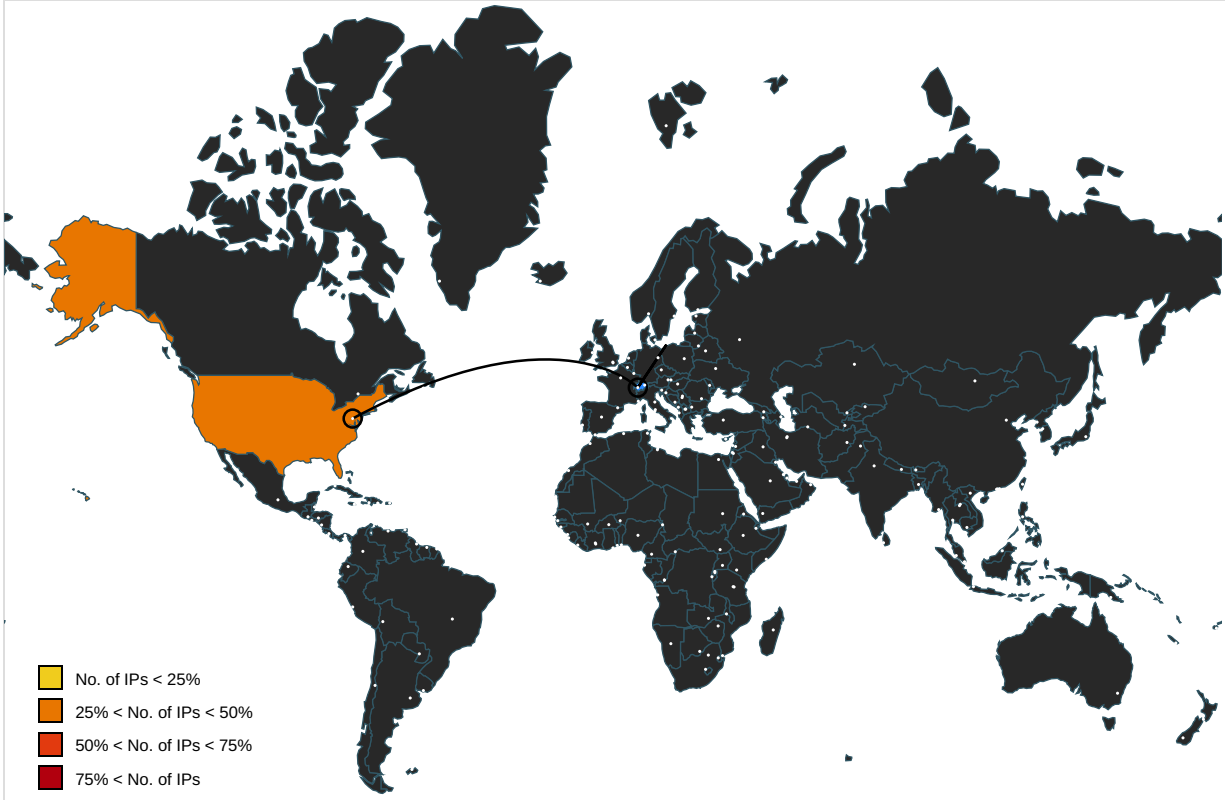
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
eu-central-7075.packetriot.net	167.71.56.116	true	true	• 10%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
eu-central-7075.packetriot.net	true	• 10%, Virustotal, Browse • Avira URL Cloud: malware	unknown
127.0.0.1	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
167.71.56.116	eu-central-7075.packetriot.net	United States		14061	DIGITALOCEAN-ASNUS	true

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	709347
Start date and time:	2022-09-25 10:37:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SdwkQEBnc3.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	20
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@1/1@12/3
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
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

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): fs.microsoft.com, login.live.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:37:58	API Interceptor	1016x Sleep call for process: SdwkQEBnc3.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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat

Process:	C:\Users\user\Desktop\SdwkQEBnc3.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Uk/tn:Ukl
MD5:	2AC74D46D23C202B8D77F932CE807595
SHA1:	E9FAFC5726FBF9B21A51370F5CB9ED07481F6C39
SHA-256:	982CB56995CCC98B0B3117C4123E053DC19903F3D41F9F3E5C036629B809E046
SHA-512:	A25513343E660EB82278A36E1B96DEA9A334F16D62D79E165EE1A9AEB49CE3AD594460161A0EEE6FD33AE5D2A94C63D758C342F421231D1669A2B5534C03562
Malicious:	**true**
Reputation:	low
Preview:	..j....H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.448162265044309
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:	SdwkQEBnc3.exe
File size:	207360
MD5:	33851c19216f0e65db0aecc27dc71ffc
SHA1:	0ad881c7d507bea247bfe454e29bc645f3d1b4ac
SHA256:	d3c3718f2106aca6ed10bb92ec37e99bcadd8536f499af4de3849625a0a1c109
SHA512:	beb70bc68603bc8722656297c7bab35fd15ba7a2d91520f22ea00b2d021ee171c38917d0ddd0bb50e752294c20bd2a257da7623c464252cde4f490c5b66af708
SSDEEP:	6144:gLV6Bta6dtJmakIM5XQa2WCE085Qe6nGH:gLV6Btpmk22Wd085GnC
TLSH:	6C14CF5677A94A2FE1DE89B9711241038378C2E7A8D3F3EF28D425B69F267E006471D3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. .....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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 byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e738	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x15d90	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
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	0x1c798	0x1c800	False	0.594495271381579	data	6.598046369910041	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x15d90	0x15e00	False	0.9997098214285715	data	7.997673261620719	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x15d38	TIM image, (2595,61413)		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3167.71.56.11649729223782025019 09/25/22-10:39:19.021240	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	22378	192.168.2.3	167.71.56.116

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3167.71.56.116 49708223782025019 09/25/22-10:37:58.335400	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49719223782025019 09/25/22-10:38:45.572488	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49728223782025019 09/25/22-10:39:13.005416	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49723223782025019 09/25/22-10:39:06.622577	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49709223782025019 09/25/22-10:38:04.391752	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49712223782025019 09/25/22-10:38:11.114012	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49723223782816766 09/25/22-10:39:08.421800	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49723	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49733223782816766 09/25/22-10:39:42.564776	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49733	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49712223782816766 09/25/22-10:38:14.198704	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49712	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49737223782025019 09/25/22-10:39:46.930085	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49716223782025019 09/25/22-10:38:33.571963	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49716	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49717223782025019 09/25/22-10:38:39.534899	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49717	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49708223782816718 09/25/22-10:37:59.384612	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49708	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49716223782816766 09/25/22-10:38:35.293304	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49716	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49737223782816766 09/25/22-10:39:48.190268	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49737	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49729223782816766 09/25/22-10:39:20.875554	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49729	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49719223782816766 09/25/22-10:38:47.309965	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49719	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49708223782816766 09/25/22-10:38:00.056144	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49717223782816766 09/25/22-10:38:41.356311	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49717	22378	192.168.2.3	167.71.56.116

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3167.71.56.116 49728223782816766 09/25/22-10:39:14.776089	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49728	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49741223782816766 09/25/22-10:39:54.862352	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49741	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49723223782816718 09/25/22-10:39:07.608396	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49723	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49733223782025019 09/25/22-10:39:40.736255	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49709223782816766 09/25/22-10:38:06.120867	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49709	22378	192.168.2.3	167.71.56.116
192.168.2.3167.71.56.116 49741223782025019 09/25/22-10:39:53.012867	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	22378	192.168.2.3	167.71.56.116

Network Port Distribution

Total Packets: 65

- 53 (DNS)
- 22378 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 25, 2022 10:37:58.264648914 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.296509027 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:58.296634912 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.335400105 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.366008043 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:58.415612936 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.446237087 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:58.477843046 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.508677006 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:58.603470087 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.635688066 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:58.673021078 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.703991890 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:58.822587967 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.855446100 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:58.883898973 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:58.914707899 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:59.009452105 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.040250063 CEST	22378	49708	167.71.56.116	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 25, 2022 10:37:59.103066921 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.133682966 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:59.320054054 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.350832939 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:59.384612083 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.415494919 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:59.468890905 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.499579906 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:59.649624109 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.680293083 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:59.712111950 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.742652893 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:59.864775896 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.895387888 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:37:59.931041002 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:37:59.961791039 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:00.056143999 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:00.127749920 CEST	22378	49708	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:00.182921886 CEST	49708	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.354166031 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.384440899 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:04.384546041 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.391752005 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.421927929 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:04.447284937 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.477539062 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:04.541570902 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.572074890 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:04.681499958 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.711612940 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:04.806596994 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.837306976 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:04.887413025 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:04.922811031 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.010030031 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.040236950 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.088083982 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.118360996 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.213840961 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.244219065 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.353310108 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.385812998 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.432198048 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.464849949 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.562103987 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.594657898 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.689172983 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.722748995 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.744601965 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.777255058 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:05.853795052 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:05.884052038 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:06.009485006 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:06.039866924 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:06.120867014 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:06.190546989 CEST	22378	49709	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:06.259795904 CEST	49709	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:10.947829008 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:10.978771925 CEST	22378	49712	167.71.56.116	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 25, 2022 10:38:10.978933096 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:11.114012003 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:11.146862030 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:11.723541021 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:11.754926920 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:11.792958021 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:11.823889971 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:11.902371883 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:11.934346914 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:11.994277000 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:12.025028944 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:12.209912062 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:12.243458033 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:12.278104067 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:12.310245037 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:13.070338964 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:13.101237059 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:13.263070107 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:13.293661118 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:13.369754076 CEST	49712	22378	192.168.2.3	167.71.56.116
Sep 25, 2022 10:38:13.400302887 CEST	22378	49712	167.71.56.116	192.168.2.3
Sep 25, 2022 10:38:13.526094913 CEST	49712	22378	192.168.2.3	167.71.56.116

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Sep 25, 2022 10:37:58.214035988 CEST	57990	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:37:58.251596928 CEST	53	57990	8.8.8.8	192.168.2.3
Sep 25, 2022 10:38:04.242063046 CEST	52387	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:38:04.352637053 CEST	53	52387	8.8.8.8	192.168.2.3
Sep 25, 2022 10:38:10.737216949 CEST	60625	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:38:10.921155930 CEST	53	60625	8.8.8.8	192.168.2.3
Sep 25, 2022 10:38:33.491652012 CEST	49302	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:38:33.538759947 CEST	53	49302	8.8.8.8	192.168.2.3
Sep 25, 2022 10:38:39.458796024 CEST	53975	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:38:39.499471903 CEST	53	53975	8.8.8.8	192.168.2.3
Sep 25, 2022 10:38:45.512289047 CEST	52955	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:38:45.532057047 CEST	53	52955	8.8.8.8	192.168.2.3
Sep 25, 2022 10:39:06.505239964 CEST	60582	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:39:06.525190115 CEST	53	60582	8.8.8.8	192.168.2.3
Sep 25, 2022 10:39:12.865638971 CEST	56042	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:39:12.972980976 CEST	53	56042	8.8.8.8	192.168.2.3
Sep 25, 2022 10:39:18.866290092 CEST	59636	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:39:18.976288080 CEST	53	59636	8.8.8.8	192.168.2.3
Sep 25, 2022 10:39:40.596112967 CEST	55638	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:39:40.703140020 CEST	53	55638	8.8.8.8	192.168.2.3
Sep 25, 2022 10:39:46.845093966 CEST	65320	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:39:46.883793116 CEST	53	65320	8.8.8.8	192.168.2.3
Sep 25, 2022 10:39:52.788522005 CEST	60767	53	192.168.2.3	8.8.8.8
Sep 25, 2022 10:39:52.979732990 CEST	53	60767	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 25, 2022 10:37:58.214035988 CEST	192.168.2.3	8.8.8.8	0x3869	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:04.242063046 CEST	192.168.2.3	8.8.8.8	0xd439	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Sep 25, 2022 10:38:10.737216949 CEST	192.168.2.3	8.8.8.8	0xce18	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:33.491652012 CEST	192.168.2.3	8.8.8.8	0xafc3	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:39.458796024 CEST	192.168.2.3	8.8.8.8	0xd21d	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:45.512289047 CEST	192.168.2.3	8.8.8.8	0xce32	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:06.505239964 CEST	192.168.2.3	8.8.8.8	0xe731	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:12.865638971 CEST	192.168.2.3	8.8.8.8	0x17be	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:18.866290092 CEST	192.168.2.3	8.8.8.8	0x8e54	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:40.596112967 CEST	192.168.2.3	8.8.8.8	0xffc4	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:46.845093966 CEST	192.168.2.3	8.8.8.8	0x1802	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:52.788522005 CEST	192.168.2.3	8.8.8.8	0xb812	Standard query (0)	eu-central-7075.packetriot.net	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Sep 25, 2022 10:37:58.251596928 CEST	8.8.8.8	192.168.2.3	0x3869	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:04.352637053 CEST	8.8.8.8	192.168.2.3	0xd439	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:10.921155930 CEST	8.8.8.8	192.168.2.3	0xce18	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:33.538759947 CEST	8.8.8.8	192.168.2.3	0xafc3	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:39.499471903 CEST	8.8.8.8	192.168.2.3	0xd21d	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:38:45.532057047 CEST	8.8.8.8	192.168.2.3	0xce32	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:06.525190115 CEST	8.8.8.8	192.168.2.3	0xe731	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:12.972980976 CEST	8.8.8.8	192.168.2.3	0x17be	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:18.976288080 CEST	8.8.8.8	192.168.2.3	0x8e54	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:40.703140020 CEST	8.8.8.8	192.168.2.3	0xffc4	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:46.883793116 CEST	8.8.8.8	192.168.2.3	0x1802	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false
Sep 25, 2022 10:39:52.979732990 CEST	8.8.8.8	192.168.2.3	0xb812	No error (0)	eu-central-7075.packetriot.net		167.71.56.116	A (IP address)	IN (0x0001)	false

Statistics

No statistics

System Behavior

Analysis Process: SdwkQEBnc3.exe PID: 5128, Parent PID: 5460

General

Target ID:	0
Start time:	10:37:56
Start date:	25/09/2022
Path:	C:\Users\user\Desktop\SdwkQEBnc3.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SdwkQEBnc3.exe"
Imagebase:	0xf10000
File size:	207360 bytes
MD5 hash:	33851C19216F0E65DB0AECC27DC71FFC
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.239926624.0000000000F12000.00000002.00000001.01000000.00000003.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.239926624.0000000000F12000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.239926624.0000000000F12000.00000002.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000000.239926624.0000000000F12000.00000002.00000001.01000000.00000003.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.511555903.0000000004637000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.511555903.0000000004637000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.511555903.0000000004637000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.513466163.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.513466163.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.513466163.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.513466163.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.513466163.0000000005E30000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.513184324.0000000005A80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.513184324.0000000005A80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.513184324.0000000005A80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.513184324.0000000005A80000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.508672696.00000000035F1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
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	729B60AC	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	729B60AC	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	5830D15	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	5830E0F	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	5830D15	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	5830D15	CreateDirectoryW
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	729B60AC	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	729B60AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SdwkQEBnc3.exe:Zone.Identifier	success or wait	1	58310B5	DeleteFileA

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	fd fd 6a fd 1c fd fd 48	jH	success or wait	1	5830FC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E8738	ReadFile
C:\Users\user\Desktop\SdwkQEBnc3.exe	unknown	4096	success or wait	1	72A8BF06	unknown
C:\Users\user\Desktop\SdwkQEBnc3.exe	unknown	512	success or wait	1	72A8BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	729E5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	5830FC7	ReadFile

Disassembly

No disassembly