ID: 626618
Sample Name: LTh59kY8ve.exe
Cookbook: default.jbs
Time: 16:22:17
Date: 14/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

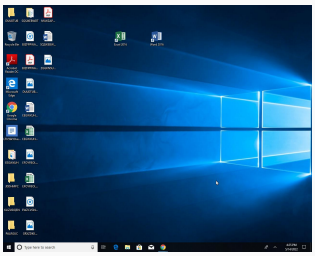
Windows Analysis Report

LTh59kY8ve.exe

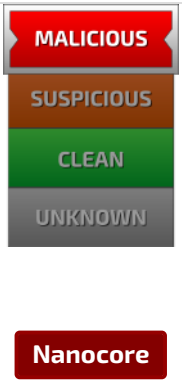
Overview

General Information

Sample Name:	LTh59kY8ve.exe
Analysis ID:	626618
MD5:	55d261de4ebfec..
SHA1:	a89750499dca36..
SHA256:	28a8b5760f88ff5..
Tags:	exe NanoCore RAT
Infos:	



Detection



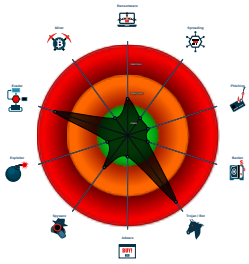
Nanocore

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Protects its processes via BreakOn…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- LTh59kY8ve.exe (PID: 6352 cmdline: "C:\Users\user\Desktop\LTh59kY8ve.exe" MD5: 55D261DE4EBFEC14610E3019BDB47E1D)
  - LTh59kY8ve.exe (PID: 6676 cmdline: {path} MD5: 55D261DE4EBFEC14610E3019BDB47E1D)
  - LTh59kY8ve.exe (PID: 6688 cmdline: {path} MD5: 55D261DE4EBFEC14610E3019BDB47E1D)
- dhcpmon.exe (PID: 6188 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 55D261DE4EBFEC14610E3019BDB47E1D)
  - dhcpmon.exe (PID: 5624 cmdline: {path} MD5: 55D261DE4EBFEC14610E3019BDB47E1D)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "b96b95d9-5642-498b-b1fc-e921a47a",
  "Group": "PUNK44",
  "Domain1": "194.5.98.208",
  "Domain2": "suchwoni13.ddns.net",
  "Port": 50720,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Enable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5009,
  "TimeoutInterval": 5008,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "1300a000",
  "GCThreshold": "1300a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.44"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000000.284589353.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000005.00000000.284589353.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000005.00000000.284589353.0000000000402000.00000040.00000400.00020000.00000000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000011.00000000.337580585.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000011.00000000.337580585.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 59 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings

Source	Rule	Description	Author	Strings
17.2.dhcpmon.exe.3099684.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0x66a6:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
17.2.dhcpmon.exe.3099684.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x66a6:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0x6784:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost • 0x66c0:$s5: IClientLoggingHost
17.2.dhcpmon.exe.3099684.3.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0x66f0:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0x66a6:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0x6706:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0x66c0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x643f:$s1: ClientPlugin • 0x66f9:$s1: ClientPlugin
17.2.dhcpmon.exe.309e6e4.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1646:$x1: NanoCore.ClientPluginHost
17.2.dhcpmon.exe.309e6e4.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1646:$x2: NanoCore.ClientPluginHost • 0x1724:$s4: PipeCreated • 0x1660:$s5: IClientLoggingHost
Click to see the 158 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208 −

Timestamp:	192.168.2.3194.5.98.2084977350720202501905/14/22-16:24:24.261336
SID:	2025019
Source Port:	49773
Destination Port:	50720
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849842507202816766 05/14/22-16:25:03.871537
SID:	2816766
Source Port:	49842
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849743507202025019 05/14/22-16:23:48.458944
SID:	2025019
Source Port:	49743
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849754507202025019 05/14/22-16:24:06.487078
SID:	2025019
Source Port:	49754
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	
Timestamp:	194.5.98.208192.168.2.350720497972841753 05/14/22-16:24:31.816886
SID:	2841753
Source Port:	50720
Destination Port:	49797
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849830507202816766 05/14/22-16:24:50.804740
SID:	2816766
Source Port:	49830
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849755507202025019 05/14/22-16:24:12.730880
SID:	2025019
Source Port:	49755
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849797507202816718 05/14/22-16:24:31.591625
SID:	2816718
Source Port:	49797
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849841507202816766 05/14/22-16:24:56.833115

SID:	2816766
Source Port:	49841
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849813507202816766 05/14/22-16:24:38.628558
SID:	2816766
Source Port:	49813
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849756507202025019 05/14/22-16:24:19.131952
SID:	2025019
Source Port:	49756
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849747507202025019 05/14/22-16:23:55.464098
SID:	2025019
Source Port:	49747
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	
Timestamp:	194.5.98.208192.168.2.350720497732841753 05/14/22-16:24:24.858130
SID:	2841753
Source Port:	50720
Destination Port:	49773
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 3 - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	
Timestamp:	194.5.98.208192.168.2.350720497472810451 05/14/22-16:23:56.023970
SID:	2810451
Source Port:	50720
Destination Port:	49747
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	
Timestamp:	194.5.98.208192.168.2.350720498502841753 05/14/22-16:25:28.467337
SID:	2841753
Source Port:	50720
Destination Port:	49850
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	
Timestamp:	194.5.98.208192.168.2.350720498132841753 05/14/22-16:24:37.808559
SID:	2841753
Source Port:	50720
Destination Port:	49813
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849816507202816766 05/14/22-16:24:44.691312
SID:	2816766
Source Port:	49816
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	
Timestamp:	194.5.98.208192.168.2.350720498162841753 05/14/22-16:24:44.881917
SID:	2841753
Source Port:	50720
Destination Port:	49816
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	
Timestamp:	194.5.98.208192.168.2.350720498412841753 05/14/22-16:24:57.057823
SID:	2841753
Source Port:	50720
Destination Port:	49841
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849849507202025019 05/14/22-16:25:21.223384
SID:	2025019
Source Port:	49849
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849849507202816766 05/14/22-16:25:22.991881
SID:	2816766
Source Port:	49849
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849797507202025019 05/14/22-16:24:30.800757
SID:	2025019
Source Port:	49797
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	
Timestamp:	194.5.98.208192.168.2.350720498302841753 05/14/22-16:24:50.885098
SID:	2841753
Source Port:	50720
Destination Port:	49830
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849753507202025019 05/14/22-16:24:00.509549

SID:	2025019
Source Port:	49753
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208

Timestamp:	192.168.2.3194.5.98.20849847507202816766 05/14/22-16:25:10.912142
SID:	2816766
Source Port:	49847
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208

Timestamp:	192.168.2.3194.5.98.20849742507202025019 05/14/22-16:23:42.118480
SID:	2025019
Source Port:	49742
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208

Timestamp:	192.168.2.3194.5.98.20849813507202025019 05/14/22-16:24:36.823454
SID:	2025019
Source Port:	49813
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208

Timestamp:	192.168.2.3194.5.98.20849773507202816766 05/14/22-16:24:25.048865
SID:	2816766
Source Port:	49773
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208

Timestamp:	192.168.2.3194.5.98.20849841507202025019 05/14/22-16:24:56.076924
SID:	2025019
Source Port:	49841
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208

Timestamp:	192.168.2.3194.5.98.20849830507202025019 05/14/22-16:24:50.008266
SID:	2025019
Source Port:	49830
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3

Timestamp:	194.5.98.208192.168.2.350720498482841753 05/14/22-16:25:16.397694
SID:	2841753
Source Port:	50720
Destination Port:	49848
Protocol:	TCP

Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849754507202816766 05/14/22-16:24:07.235648
SID:	2816766
Source Port:	49754
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849848507202025019 05/14/22-16:25:16.140253
SID:	2025019
Source Port:	49848
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849743507202816766 05/14/22-16:23:50.178691
SID:	2816766
Source Port:	49743
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849797507202816766 05/14/22-16:24:31.591625
SID:	2816766
Source Port:	49797
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849816507202025019 05/14/22-16:24:43.894956
SID:	2025019
Source Port:	49816
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849742507202816766 05/14/22-16:23:43.150017
SID:	2816766
Source Port:	49742
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849753507202816766 05/14/22-16:24:01.234848
SID:	2816766
Source Port:	49753
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	
Timestamp:	192.168.2.3194.5.98.20849847507202025019 05/14/22-16:25:09.165823

SID:	2025019
Source Port:	49847
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	−
Timestamp:	192.168.2.3194.5.98.20849850507202025019 05/14/22-16:25:28.236978
SID:	2025019
Source Port:	49850
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	−
Timestamp:	194.5.98.208192.168.2.350720497532841753 05/14/22-16:24:01.459957
SID:	2841753
Source Port:	50720
Destination Port:	49753
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	−
Timestamp:	194.5.98.208192.168.2.350720497542841753 05/14/22-16:24:07.445297
SID:	2841753
Source Port:	50720
Destination Port:	49754
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	−
Timestamp:	192.168.2.3194.5.98.20849755507202816766 05/14/22-16:24:13.856596
SID:	2816766
Source Port:	49755
Destination Port:	50720
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	−
Timestamp:	194.5.98.208192.168.2.350720497562841753 05/14/22-16:24:19.458362
SID:	2841753
Source Port:	50720
Destination Port:	49756
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 194.5.98.208 - Destination IP: 192.168.2.3	−
Timestamp:	194.5.98.208192.168.2.350720497472841753 05/14/22-16:23:56.023970
SID:	2841753
Source Port:	50720
Destination Port:	49747
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 194.5.98.208	−
Timestamp:	192.168.2.3194.5.98.20849842507202025019 05/14/22-16:25:02.076779
SID:	2025019
Source Port:	49842
Destination Port:	50720
Protocol:	TCP

Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

Operating System Destruction

Protects its processes via BreakOnTermination flag

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

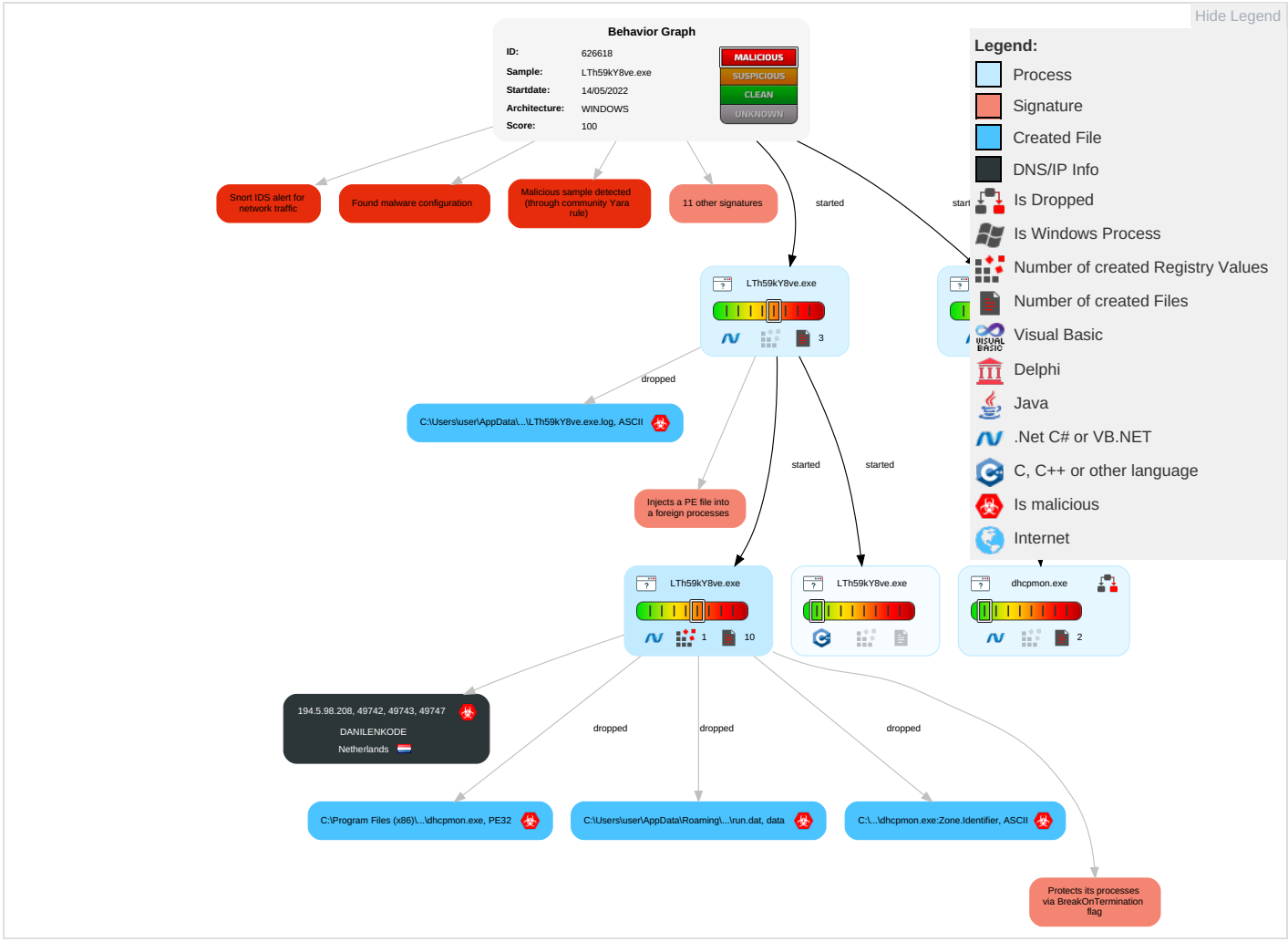
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 1 2 Process Injection	2 Masquerading	1 1 Input Capture	2 1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 3 Software Packing	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

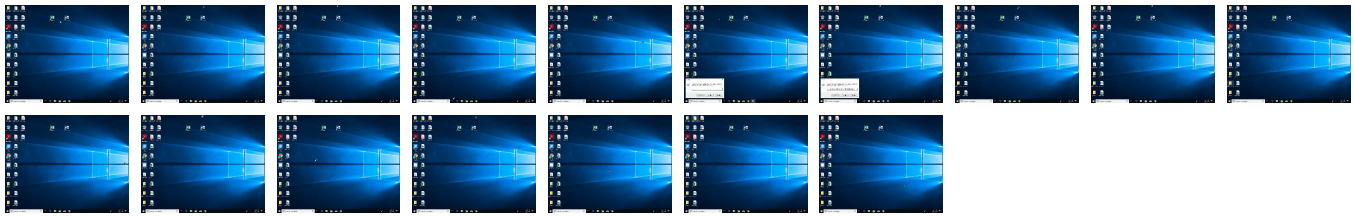
Behavior Graph



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
LTh59kY8ve.exe	55%	Virustotal		Browse
LTh59kY8ve.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
LTh59kY8ve.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	55%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	66%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.LTh59kY8ve.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.LTh59kY8ve.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
17.0.dhcpmon.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.LTh59kY8ve.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.LTh59kY8ve.exe.5d70000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
17.0.dhcpmon.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.LTh59kY8ve.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.LTh59kY8ve.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.0.LTh59kY8ve.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.dhcpmon.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.dhcpmon.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
17.0.dhcpmon.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
suchwoni13.ddns.net	5%	Virustotal		Browse
suchwoni13.ddns.net	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
194.5.98.208	2%	Virustotal		Browse
194.5.98.208	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
suchwoni13.ddns.net	true	• 5%, Virustotal, Browse • Avira URL Cloud: safe	unknown

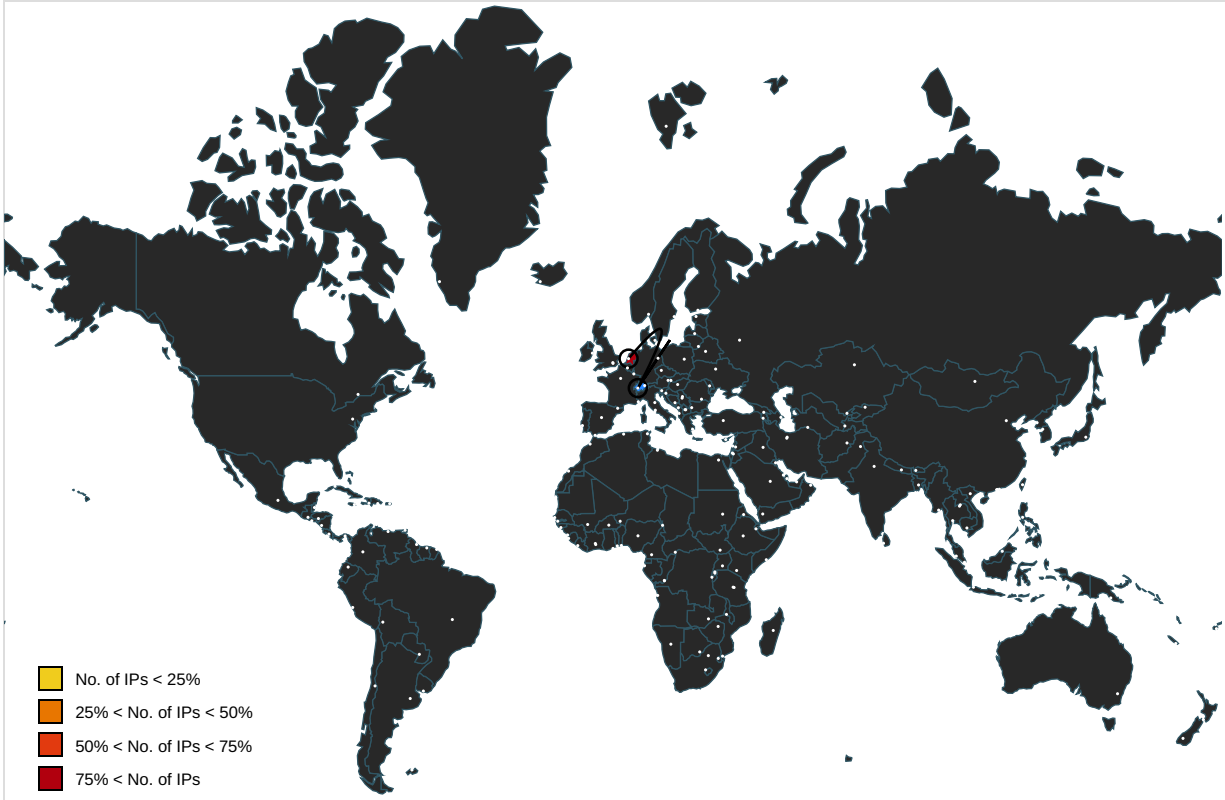
Name	Malicious	Antivirus Detection	Reputation
194.5.98.208	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.urwpp.deDPlease	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	LTh59kY8ve.exe, 00000005.00000002.516655069.00000000029D1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	LTh59kY8ve.exe, 00000000.00000002.296223060.0000000007072000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
194.5.98.208	unknown	Netherlands		208476	DANILENKODE	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	626618
Start date and time: 14/05/202216:22:17	2022-05-14 16:22:17 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LTh59kY8ve.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	28
Number of new started drivers analysed:	0
Number of existing processes analysed:	0

Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@8/6@0/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 13.3% (good quality ratio 6.2%) • Quality average: 31.2% • Quality standard deviation: 40.2%
HCA Information:	• Successful, ratio: 92% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Execution Graph export aborted for target LTh59kY8ve.exe, PID 6676 because there are no executed function
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:23:29	API Interceptor	908x Sleep call for process: LTh59kY8ve.exe modified
16:23:42	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
16:23:57	API Interceptor	2x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\LTh59kY8ve.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	678912
Entropy (8bit):	7.46600430601963
Encrypted:	false
SSDEEP:	12288:PgjjnsWrKXykpGef2zbffLgACRlVXFFssGbsQA7iefH2zM36m:PgjjndrKzpnuffL4Rr
MD5:	55D261DE4EBFEC14610E3019BDB47E1D
SHA1:	A89750499DCA367037B9388A820E8FB56CD2F3BB
SHA-256:	28A8B5760F88FF56FCCAC79F506AA87DE847161F5B3AF7158792D098A60785DD
SHA-512:	1866B89A217F81DE6B106A6094E526A872380BA35F45D83D74CA890DD97DA331E127F5007B7E194E06B85B74866948F950FBFF17773442E664FB0A364D2B339E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 55%, Browse • Antivirus: ReversingLabs, Detection: 66%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....nxb.....P..J.....h... .....@.. ..@.....h..O.....`..... ..... ..H.....text....H... ...J..... ..`.rsrc...`.....L.....@..@.rel oc.....Z.....@..B.....h.....H.....Q..h/.....*..(#...*..($...*.s%.....s&.....s'.....s(.....s).....*.~....o*...*.~....o+...*.~.. ..o,...*.~....o-...*.~....o....*R.....o1.....*..(2...*6..($...(%...*..(&...*.....(....*..('...*b..{....(...+}.....{....*b..{....(...+}.....{....*b..{....(...+}.....{....*b..{....(...+}.....{....*...{.....,.rq..p((...z..|....(...+*...{.....,.rq..p((...z..|....(...+*...{.....,.rq..p((...z..|....(.

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

Process:	C:\Users\user\Desktop\LTh59kY8ve.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LTh59kY8ve.exe.log

Process:	C:\Users\user\Desktop\LTh59kY8ve.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**

Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F F8
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

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

Process:	C:\Users\user\Desktop\LTh59kY8ve.exe
File Type:	data
Category:	modified
Size (bytes):	128
Entropy (8bit):	6.527114648336088
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRH5/ljRAaTlKYrI1Sj9txROIsxcMek2:X4LDAn1rplKTYBROIsxek2
MD5:	0A9C5EAE8756D6FC90F59D8D71A79E1E
SHA1:	0F7D6AAED17CD18DC614535ED26335C147E29ED7
SHA-256:	B1921EA14C66927397BAF3FA456C22B93C30C3DE23546087C0B18551CE5001C5
SHA-512:	78C2F399AC49C78D89915DFF99AC955B5E0AB07BAAD61B07B0CE073C88C1D3A9F1D302C2413691B349DD34441B0FF909C08A4F71E2F1B73F46C1FF308BC7CF A
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P.OT....g.t.....'7.....)..8zII..K/....n3...3.5.....&.7].)..wL...:}g...@...mV.....JUP...w

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

Process:	C:\Users\user\Desktop\LTh59kY8ve.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:tVxt:T
MD5:	A533435182F3D3AED03CC612AB803E0E
SHA1:	814F1CDA8B9656B504509CA90FE1E27AF249E9E9
SHA-256:	84048C7CFFABB495AF9B44BD25EC50D2BBC8F071CF399A91F14184BAE3CE41D4
SHA-512:	08A6DBB9C32F1C813D36DF3BF8BAD5976698831B155D2E391AF6F51695DB4FFA5A112F43BDE4775F6936BB6DAD5F879DA87640B831F190B14D7045193DC42B9
Malicious:	**true**
Reputation:	low

Preview:	....6.H

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.46600430601963
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	LTh59kY8ve.exe
File size:	678912
MD5:	55d261de4ebfec14610e3019bdb47e1d
SHA1:	a89750499dca367037b9388a820e8fb56cd2f3bb
SHA256:	28a8b5760f88ff56fccac79f506aa87de847161f5b3af7158792d098a60785dd
SHA512:	1866b89a217f81de6b106a6094e526a872380ba35f45d83d74ca890dd97da331e127f5007b7e194e06b85b74866948f950fbff17773442e664fb0a364d2b339e
SSDEEP:	12288:PgjjnsWrKXykpGef2zbffLgACRlVXFFssGbsQA7iefH2zM36m:PgjjndrKzpnuffL4Rr
TLSH:	94E428B8F120649EF45BF471CD682C5795916E6AC31A42025C23F3B95E7E6F28E10CBE
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.......PE..L....nxb.....P..J.....h... .....@.. .....@.....

File Icon

Icon Hash:	01e0c4c4c4c4d803

Static PE Info

General

Entrypoint:	0x4968ee
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x62786E1A [Mon May 9 01:27:54 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x9689c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x98000	0x10c60	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xaa000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x948f4	0x94a00	False	0.800051908116	data	7.65039354316	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x98000	0x10c60	0x10e00	False	0.0299045138889	data	3.07392434961	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0xaa000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x980e8	0x10828	data		
RT_GROUP_ICON	0xa8910	0x14	data		
RT_VERSION	0xa8924	0x33c	data		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright CPT185
Assembly Version	1.2.0.0
InternalName	FEttW74.exe
FileVersion	1.2.0.0
CompanyName	CPT185
LegalTrademarks	
Comments	
ProductName	CPT185_Homework
ProductVersion	1.2.0.0
FileDescription	CPT185_Homework
OriginalFilename	FEttW74.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3194.5.98.2084977350720202501905/14/22-16:24:24.261336	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49773	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084984250720281676605/14/22-16:25:03.871537	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49842	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084974350720202501905/14/22-16:23:48.458944	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084975450720202501905/14/22-16:24:06.487078	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	50720	192.168.2.3	194.5.98.208
194.5.98.208192.168.2.350720497972841753305/14/22-16:24:31.816886	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49797	194.5.98.208	192.168.2.3
192.168.2.3194.5.98.2084983050720281676605/14/22-16:24:50.804740	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49830	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084975550720202501905/14/22-16:24:12.730880	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	50720	192.168.2.3	194.5.98.208

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3194.5.98.2084 9797507202816718 05/14/22-16:24:31.591625	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49797	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9841507202816766 05/14/22-16:24:56.833115	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49841	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9813507202816766 05/14/22-16:24:38.628558	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49813	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9756507202025019 05/14/22-16:24:19.131952	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9747507202025019 05/14/22-16:23:55.464098	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	50720	192.168.2.3	194.5.98.208
194.5.98.208192.168.2.35 0720497732841753 05/14/22-16:24:24.858130	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49773	194.5.98.208	192.168.2.3
194.5.98.208192.168.2.35 0720497472810451 05/14/22-16:23:56.023970	TCP	2810451	ETPRO TROJAN NanoCore RAT Keepalive Response 3	50720	49747	194.5.98.208	192.168.2.3
194.5.98.208192.168.2.35 0720498502841753 05/14/22-16:25:28.467337	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49850	194.5.98.208	192.168.2.3
194.5.98.208192.168.2.35 0720498132841753 05/14/22-16:24:37.808559	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49813	194.5.98.208	192.168.2.3
192.168.2.3194.5.98.2084 9816507202816766 05/14/22-16:24:44.691312	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49816	50720	192.168.2.3	194.5.98.208
194.5.98.208192.168.2.35 0720498162841753 05/14/22-16:24:44.881917	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49816	194.5.98.208	192.168.2.3
194.5.98.208192.168.2.35 0720498412841753 05/14/22-16:24:57.057823	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49841	194.5.98.208	192.168.2.3
192.168.2.3194.5.98.2084 9849507202025019 05/14/22-16:25:21.223384	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49849	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9849507202816766 05/14/22-16:25:22.991881	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49849	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9797507202025019 05/14/22-16:24:30.800757	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	50720	192.168.2.3	194.5.98.208
194.5.98.208192.168.2.35 0720498302841753 05/14/22-16:24:50.885098	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49830	194.5.98.208	192.168.2.3
192.168.2.3194.5.98.2084 9753507202025019 05/14/22-16:24:00.509549	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9847507202816766 05/14/22-16:25:10.912142	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49847	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9742507202025019 05/14/22-16:23:42.118480	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	50720	192.168.2.3	194.5.98.208

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3194.5.98.2084 9813507202025019 05/14/22-16:24:36.823454	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9773507202816766 05/14/22-16:24:25.048865	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49773	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9841507202025019 05/14/22-16:24:56.076924	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49841	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9830507202025019 05/14/22-16:24:50.008266	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49830	50720	192.168.2.3	194.5.98.208
194.5.98.208192.168.2.35 0720498482841753 05/14/22-16:25:16.397694	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49848	194.5.98.208	192.168.2.3
192.168.2.3194.5.98.2084 9754507202816766 05/14/22-16:24:07.235648	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49754	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9848507202025019 05/14/22-16:25:16.140253	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49848	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9743507202816766 05/14/22-16:23:50.178691	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49743	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9797507202816766 05/14/22-16:24:31.591625	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49797	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9816507202025019 05/14/22-16:24:43.894956	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49816	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9742507202816766 05/14/22-16:23:43.150017	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49742	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9753507202816766 05/14/22-16:24:01.234848	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49753	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9847507202025019 05/14/22-16:25:09.165823	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49847	50720	192.168.2.3	194.5.98.208
192.168.2.3194.5.98.2084 9850507202025019 05/14/22-16:25:28.236978	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49850	50720	192.168.2.3	194.5.98.208
194.5.98.208192.168.2.35 0720497532841753 05/14/22-16:24:01.459957	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49753	194.5.98.208	192.168.2.3
194.5.98.208192.168.2.35 0720497542841753 05/14/22-16:24:07.445297	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49754	194.5.98.208	192.168.2.3
192.168.2.3194.5.98.2084 9755507202816766 05/14/22-16:24:13.856596	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49755	50720	192.168.2.3	194.5.98.208
194.5.98.208192.168.2.35 0720497562841753 05/14/22-16:24:19.458362	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49756	194.5.98.208	192.168.2.3
194.5.98.208192.168.2.35 0720497472841753 05/14/22-16:23:56.023970	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	50720	49747	194.5.98.208	192.168.2.3

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3194.5.98.2084984250720202501905/14/22-16:25:02.076779	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	50720	192.168.2.3	194.5.98.208

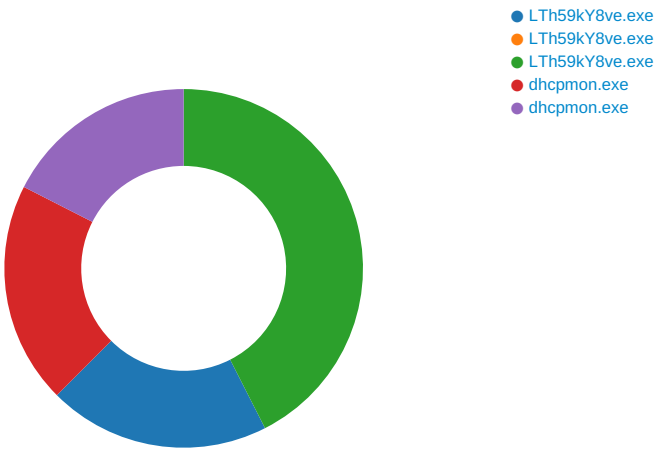
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 16:23:41.705560923 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:41.930619955 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:41.930820942 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:42.118479967 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:42.500293970 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:42.501665115 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:42.924268007 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:42.924472094 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:43.149785042 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:43.150017023 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:43.630467892 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:43.630755901 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:43.909239054 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:43.909300089 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:43.909429073 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:44.137768984 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.138129950 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.138992071 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:44.139049053 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.139091015 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.141625881 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:44.145737886 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:44.364311934 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.364512920 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:44.364692926 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.364761114 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:44.365200996 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.365243912 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.365314960 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:44.366807938 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.367191076 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.367321968 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:44.367496014 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.367702007 CEST	50720	49742	194.5.98.208	192.168.2.3
May 14, 2022 16:23:44.367775917 CEST	49742	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:48.202945948 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:48.457214117 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:48.457416058 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:48.458944082 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:48.782872915 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:48.783123016 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:49.008555889 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:49.061130047 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:49.202789068 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:49.688108921 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:49.754642010 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.084530115 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.084947109 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.085200071 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.178690910 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.314474106 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.314538002 CEST	50720	49743	194.5.98.208	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 14, 2022 16:23:50.314732075 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.314763069 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.314806938 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.314826012 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.318109035 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.557126999 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.557183981 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.557272911 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.565356016 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.586791039 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.586843967 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.586909056 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.586992979 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.587068081 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.587110043 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.587125063 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.587166071 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.783198118 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.783265114 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.783303976 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.783338070 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.783343077 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.783400059 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.813695908 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.816730022 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.816787004 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.816826105 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.816859007 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.816898108 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.816941977 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.817074060 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.817128897 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.817152023 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.817441940 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.817502975 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.817992926 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.818973064 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.819062948 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.819165945 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:50.819359064 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:50.819434881 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:51.009120941 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:51.009263039 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:51.009288073 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:51.009320974 CEST	49743	50720	192.168.2.3	194.5.98.208
May 14, 2022 16:23:51.009517908 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:51.009541988 CEST	50720	49743	194.5.98.208	192.168.2.3
May 14, 2022 16:23:51.009572029 CEST	49743	50720	192.168.2.3	194.5.98.208

Statistics

Behavior



System Behavior

Analysis Process: LTh59kY8ve.exe PID: **6352**, Parent PID: **5668**

General

Target ID:	0
Start time:	16:23:19
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\LTh59kY8ve.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\LTh59kY8ve.exe"
Imagebase:	0xad0000
File size:	678912 bytes
MD5 hash:	55D261DE4EBFEC14610E3019BDB47E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.292121515.0000000003F59000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.292121515.0000000003F59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.292121515.0000000003F59000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDCCF06	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	6DDCCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LTh59kY8ve.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E0DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\LTh59kY8ve.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E0DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC11B4F	ReadFile

Analysis Process: LTh59kY8ve.exe PID: **6676**, Parent PID: **6352**

General

Target ID:	4
Start time:	16:23:31
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\LTh59kY8ve.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x2b0000
File size:	678912 bytes
MD5 hash:	55D261DE4EBFEC14610E3019BDB47E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	low

Analysis Process: LTh59kY8ve.exe PID: **6688**, Parent PID: **6352**

General

Target ID:	5
Start time:	16:23:32
Start date:	14/05/2022
Path:	C:\Users\user\Desktop\LTh59kY8ve.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x520000
File size:	678912 bytes
MD5 hash:	55D261DE4EBFEC14610E3019BDB47E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.284589353.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.284589353.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.284589353.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.281492315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.281492315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.281492315.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.519202292.0000000005430000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.519202292.0000000005430000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000005.00000002.519202292.0000000005430000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.284956810.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.284956810.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.284956810.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.519044938.0000000005210000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.519044938.0000000005210000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000005.00000002.519044938.0000000005210000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.519328532.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000005.00000002.519328532.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.519328532.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000005.00000002.519328532.0000000005D70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000002.514448487.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.514448487.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.514448487.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.517646825.00000000039D9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.517646825.00000000039D9000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000005.00000000.284092405.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000000.284092405.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000000.284092405.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.516655069.00000000029D1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDCCF06	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	6DDCCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6CC11E60	CreateFileW
C:\Program Files (x86)\DHCP 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	6CC1BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.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	6CC1DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CC1DD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CC1BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	15	6CC11E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	a4 fd fd 00 36 fd 48	6H	success or wait	1	6CC11B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	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 1a 6e 78 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 50 00 00 4a 09 00 00 10 01 00 00 00 00 00 fd 68 09 00 00 20 00 00 00 fd 09 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0a 00 00 02 00 00 00 00 00 00 02 00 40 fd 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.$PELnxbPJh @ @	success or wait	3	6CC1DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6CC1DD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	128	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 4f 54 fd fd fd fd 67 fd 74 1d fd fd fd fd 14 27 37 fd 1c fd fd fd fd 29 85 fd 38 7a 49 49 7a fd 4b 2f 1e fd 0e fd 6e 33 10 fd fd 33 fd 35 fd fd 07 fd fd fd fd 26 fd 37 5d fd 29 fd fd 77 4c fd fd fd 3a 7d 67 09 fd 2e 40 fd fd fd 6d 56 72 fd fd fd fd 4a 55 50 fd fd fd 77	Gjh\3A5x&i+c(1POTgt'7)8zIIK/n3 35&7])wL:}g.@mVJUPw	success or wait	15	6CC11B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC11B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6DD8D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6DD8D72F	unknown
C:\Users\user\Desktop\LTh59kY8ve.exe	unknown	4096	success or wait	1	6DD8D72F	unknown
C:\Users\user\Desktop\LTh59kY8ve.exe	unknown	512	success or wait	1	6DD8D72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	6DD8D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DD8D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	6DD8D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6CC1646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **6188**, Parent PID: **3968**

General

Target ID:	15
Start time:	16:23:51
Start date:	14/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x6a0000
File size:	678912 bytes
MD5 hash:	55D261DE4EBFEC14610E3019BDB47E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.345719684.0000000003A19000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.345719684.0000000003A19000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.345719684.0000000003A19000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 55%, Virustotal, Browse • Detection: 66%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDCCF06	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	6DDCCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E0DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E0DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC11B4F	ReadFile

Analysis Process: dhcpmon.exe PID: **5624**, Parent PID: **6188**

General

Target ID:	17
Start time:	16:24:00
Start date:	14/05/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xca0000
File size:	678912 bytes
MD5 hash:	55D261DE4EBFEC14610E3019BDB47E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.337580585.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.337580585.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.337580585.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.339572272.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.339572272.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.339572272.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.358359807.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.358359807.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.358359807.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.338758899.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.338758899.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.338758899.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.361079105.0000000003031000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.361079105.0000000003031000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000000.339186233.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.339186233.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.339186233.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.361375815.0000000004039000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.361375815.0000000004039000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6DDCCF06	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	6DDCCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DDA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DD003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DD003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DDA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CC11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CC11B4F	ReadFile

Disassembly

No disassembly