ID: 796483
Sample Name: Quote No 2118013.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 22:32:21
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

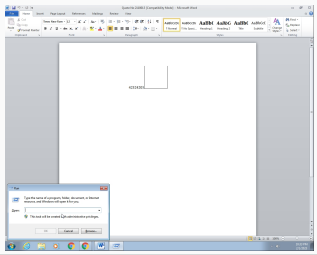
Windows Analysis Report

Quote No 2118013.doc

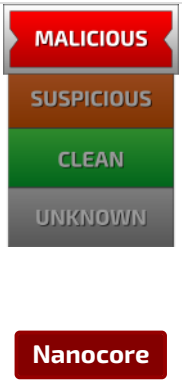
Overview

General Information

Sample Name:	Quote No 2118013.doc
Analysis ID:	796483
MD5:	342550e9ccd1…
SHA1:	30f28411b298a..
SHA256:	9ab75f3c60adc..
Tags:	CVE-2017-11882 doc NanoCore
Infos:	



Detection



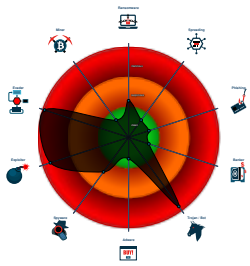
Nanocore

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

Signatures

- Sigma detected: EQNEDT32.EXE c…
- Detected unpacking (overwrites its o…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: File Dropped By EQ…
- Multi AV Scanner detection for drop…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 2876 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 3000 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - word.exe (PID: 2848 cmdline: C:\Users\user\AppData\Roaming\word.exe MD5: D3E933B0AAB571BDC73355A106D657E0)
    - rnixgfly.exe (PID: 2036 cmdline: "C:\Users\user\AppData\Local\Temp\rnixgfly.exe" C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt MD5: C1DC97853E14C21B463C6E95B21C300C)
      - rnixgfly.exe (PID: 2116 cmdline: C:\Users\user\AppData\Local\Temp\rnixgfly.exe MD5: C1DC97853E14C21B463C6E95B21C300C)
- jfcarlsrvb.exe (PID: 2216 cmdline: "C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe" "C:\Users\user\AppData\Local\Temp\rnixgfly.exe" C:\Users\user\AppData\Lo MD5: C1DC97853E14C21B463C6E95B21C300C)
- EQNEDT32.EXE (PID: 1972 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7dcf7c5d-e4be-40f9-826b-505d4386",
  "Group": "Inflows",
  "Domain1": "boele.duckdns.org",
  "Domain2": "boele.duckdns.org",
  "Port": 6269,
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
Quote No 2118013.doc	SUSP_INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embedding one of the object mostly observed in exploit (e.g. CVE-2017-11882) documents.	ditekSHen	• 0x6b:$obj2: \objdata • 0x22d:$obj3: \objupdate • 0x46:$obj6: \objlink
Quote No 2118013.doc	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x6b:$obj2: \objdata • 0x22d:$obj3: \objupdate • 0x46:$obj6: \objlink

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.1188366670.00000000065A0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x39eb:$x1: NanoCore.ClientPluginHost • 0x3a24:$x2: IClientNetworkHost
00000007.00000002.1188366670.00000000065A0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x39eb:$x2: NanoCore.ClientPluginHost • 0x3b36:$s4: PipeCreated • 0x3a05:$s5: IClientLoggingHost
00000007.00000002.1188366670.00000000065A0000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x3a8b:$x2: NanoCore.ClientPlugin • 0x39eb:$x3: NanoCore.ClientPluginHost • 0x3aa1:$i3: IClientNetwork • 0x3a43:$i5: IClientDataHost • 0x3a05:$i6: IClientLoggingHost • 0x3a24:$i7: IClientNetworkHost • 0x426c:$i9: IClientNameObjectCollection • 0x3741:$s1: ClientPlugin • 0x3a94:$s1: ClientPlugin • 0x4680:$s2: EndPoint • 0x4371:$s3: IPAddress • 0x3c83:$s4: IPEndPoint • 0x43a3:$s7: get_Connected

Source	Rule	Description	Author	Strings
00000007.00000002.1188366670.00000000065A0000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x39eb:$a1: NanoCore.ClientPluginHost • 0x3a8b:$a2: NanoCore.ClientPlugin • 0x47e1:$b7: LogClientException • 0x3a05:$b9: IClientLoggingHost
00000007.00000002.1188464789.00000000065D0000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x1f1db:$x1: NanoCore.ClientPluginHost • 0x1f1f5:$x2: IClientNetworkHost
Click to see the 98 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.rnixgfly.exe.46b0000.18.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
7.2.rnixgfly.exe.46b0000.18.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
7.2.rnixgfly.exe.46b0000.18.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xe38:$x2: NanoCore.ClientPlugin • 0xe75:$x3: NanoCore.ClientPluginHost • 0xe5a:$i1: IClientApp • 0xe4e:$i2: IClientData • 0xe29:$i3: IClientNetwork • 0xec3:$i4: IClientAppHost • 0xe65:$i5: IClientDataHost • 0xeb0:$i6: IClientLoggingHost • 0xe8f:$i7: IClientNetworkHost • 0xea2:$i8: IClientUIHost • 0xed2:$i9: IClientNameObjectCollection • 0xef7:$i10: IClientReadOnlyNameObjectCollection • 0xe41:$s1: ClientPlugin • 0x177c:$s1: ClientPlugin • 0x1789:$s1: ClientPlugin • 0x11f9:$s6: get_ClientSettings • 0x1249:$s7: get_Connected
7.2.rnixgfly.exe.46b0000.18.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xe75:$a1: NanoCore.ClientPluginHost • 0xe38:$a2: NanoCore.ClientPlugin • 0x120c:$b1: get_BuilderSettings • 0xec3:$b4: IClientAppHost • 0x127d:$b6: AddHostEntry • 0x12ec:$b7: LogClientException • 0x1261:$b8: PipeExists • 0xeb0:$b9: IClientLoggingHost
7.2.rnixgfly.exe.56f0000.24.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x16e3:$x1: NanoCore.ClientPluginHost • 0x171c:$x2: IClientNetworkHost
Click to see the 288 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920062692816766 02/01/23-22:34:43.189770
SID:	2816766
Source Port:	49200
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919262692816766 02/01/23-22:34:05.557258
SID:	2816766
Source Port:	49192
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324918862692025019 02/01/23-22:33:46.711822
SID:	2025019
Source Port:	49188
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269492082841753 02/01/23-22:35:24.322607
SID:	2841753
Source Port:	6269
Destination Port:	49208
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920362692816766 02/01/23-22:34:58.588930
SID:	2816766
Source Port:	49203
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920662692025019 02/01/23-22:35:14.040549
SID:	2025019
Source Port:	49206
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324918562692816766 02/01/23-22:33:42.424345
SID:	2816766
Source Port:	49185
Destination Port:	6269

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919062692816718 02/01/23-22:33:56.804784
SID:	2816718
Source Port:	49190
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920162692025019 02/01/23-22:34:48.135847
SID:	2025019
Source Port:	49201
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920162692816718 02/01/23-22:34:48.213161
SID:	2816718
Source Port:	49201
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919562692816766 02/01/23-22:34:21.457259
SID:	2816766
Source Port:	49195
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919362692025019 02/01/23-22:34:10.437260
SID:	2025019
Source Port:	49193
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324918362692025019 02/01/23-22:33:33.655639
SID:	2025019
Source Port:	49183
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920862692816766 02/01/23-22:35:24.406415
SID:	2816766
Source Port:	49208
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.132491826269281676 6 02/01/23-22:33:29.150304
SID:	2816766
Source Port:	49182
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.132492056269281676 6 02/01/23-22:35:09.135573
SID:	2816766
Source Port:	49205
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.132491846269281676 6 02/01/23-22:33:38.036128
SID:	2816766
Source Port:	49184
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.132491946269281676 6 02/01/23-22:34:17.104190
SID:	2816766
Source Port:	49194
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22

Timestamp:	45.137.65.132192.168.2.226269491832841753 02/01/23-22:33:33.694801
SID:	2841753
Source Port:	6269
Destination Port:	49183
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.132491926269202501 9 02/01/23-22:34:05.362301
SID:	2025019
Source Port:	49192
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.132491996269202501 9 02/01/23-22:34:38.766002
SID:	2025019
Source Port:	49199
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.132492046269202501 9 02/01/23-22:35:03.284314
SID:	2025019
Source Port:	49204
Destination Port:	6269

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269491982841753 02/01/23-22:34:34.472656
SID:	2841753
Source Port:	6269
Destination Port:	49198
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919062692025019 02/01/23-22:33:56.681631
SID:	2025019
Source Port:	49190
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919362692816766 02/01/23-22:34:11.683759
SID:	2816766
Source Port:	49193
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269491892841753 02/01/23-22:33:52.332924
SID:	2841753
Source Port:	6269
Destination Port:	49189
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269492002841753 02/01/23-22:34:43.093025
SID:	2841753
Source Port:	6269
Destination Port:	49200
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324918962692025019 02/01/23-22:33:52.298886
SID:	2025019
Source Port:	49189
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919862692025019 02/01/23-22:34:34.436858
SID:	2025019
Source Port:	49198
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22

Timestamp:	45.137.65.132192.168.2.226269491852841753 02/01/23-22:33:42.356276
SID:	2841753
Source Port:	6269
Destination Port:	49185
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	−
Timestamp:	45.137.65.132192.168.2.226269491962841753 02/01/23-22:34:25.705442
SID:	2841753
Source Port:	6269
Destination Port:	49196
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	−
Timestamp:	45.137.65.132192.168.2.226269491902841753 02/01/23-22:33:56.719131
SID:	2841753
Source Port:	6269
Destination Port:	49190
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	−
Timestamp:	45.137.65.132192.168.2.226269491922841753 02/01/23-22:34:05.398117
SID:	2841753
Source Port:	6269
Destination Port:	49192
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.1324920362692025019 02/01/23-22:34:58.374868
SID:	2025019
Source Port:	49203
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.1324920662692816766 02/01/23-22:35:14.483677
SID:	2816766
Source Port:	49206
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.1324918962692816766 02/01/23-22:33:52.436607
SID:	2816766
Source Port:	49189
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.1324919162692025019 02/01/23-22:34:01.037424
SID:	2025019
Source Port:	49191
Destination Port:	6269

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919662692816766 02/01/23-22:34:25.729294
SID:	2816766
Source Port:	49196
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919962692816766 02/01/23-22:34:38.834547
SID:	2816766
Source Port:	49199
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919462692025019 02/01/23-22:34:16.062227
SID:	2025019
Source Port:	49194
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324918462692025019 02/01/23-22:33:37.918139
SID:	2025019
Source Port:	49184
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324918362692816766 02/01/23-22:33:33.792254
SID:	2816766
Source Port:	49183
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920262692025019 02/01/23-22:34:53.384126
SID:	2025019
Source Port:	49202
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920862692025019 02/01/23-22:35:24.288274
SID:	2025019
Source Port:	49208
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.1324920762692816766 02/01/23-22:35:20.080067
SID:	2816766
Source Port:	49207
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.1324919762692025019 02/01/23-22:34:30.147504
SID:	2025019
Source Port:	49197
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22

Timestamp:	45.137.65.132192.168.2.226269491932810290 02/01/23-22:34:11.805752
SID:	2810290
Source Port:	6269
Destination Port:	49193
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.1324920562692025019 02/01/23-22:35:08.089961
SID:	2025019
Source Port:	49205
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.1324920462692816766 02/01/23-22:35:03.782867
SID:	2816766
Source Port:	49204
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.1324920062692025019 02/01/23-22:34:43.058807
SID:	2025019
Source Port:	49200
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.1324920762692025019 02/01/23-22:35:18.957271
SID:	2025019
Source Port:	49207
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132

Timestamp:	192.168.2.2245.137.65.1324921062692025019 02/01/23-22:35:28.658958
SID:	2025019
Source Port:	49210
Destination Port:	6269

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269491842841753 02/01/23-22:33:37.953540
SID:	2841753
Source Port:	6269
Destination Port:	49184
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919662692025019 02/01/23-22:34:25.668610
SID:	2025019
Source Port:	49196
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919762692816766 02/01/23-22:34:30.191917
SID:	2816766
Source Port:	49197
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324919162692816766 02/01/23-22:34:01.259922
SID:	2816766
Source Port:	49191
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324920162692816766 02/01/23-22:34:48.556940
SID:	2816766
Source Port:	49201
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	
Timestamp:	192.168.2.2245.137.65.1324918562692025019 02/01/23-22:33:42.320152
SID:	2025019
Source Port:	49185
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269492102841753 02/01/23-22:35:28.695632
SID:	2841753
Source Port:	6269
Destination Port:	49210
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22

Timestamp:	45.137.65.132192.168.2.226269491882841753 02/01/23-22:33:46.748199
SID:	2841753
Source Port:	6269
Destination Port:	49188
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.132491956269202501 9 02/01/23-22:34:21.323516
SID:	2025019
Source Port:	49195
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.132491986269281676 6 02/01/23-22:34:34.560423
SID:	2816766
Source Port:	49198
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	−
Timestamp:	45.137.65.132192.168.2.226269492032841753 02/01/23-22:34:58.443751
SID:	2841753
Source Port:	6269
Destination Port:	49203
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.132492026269281676 6 02/01/23-22:34:53.943308
SID:	2816766
Source Port:	49202
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.132491906269281676 6 02/01/23-22:33:56.804784
SID:	2816766
Source Port:	49190
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.22 - Destination IP: 45.137.65.132	−
Timestamp:	192.168.2.2245.137.65.132491886269281676 6 02/01/23-22:33:46.773305
SID:	2816766
Source Port:	49188
Destination Port:	6269
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	−
Timestamp:	45.137.65.132192.168.2.226269491972841753 02/01/23-22:34:30.181373
SID:	2841753
Source Port:	6269
Destination Port:	49197

Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269491992841753 02/01/23-22:34:38.800055
SID:	2841753
Source Port:	6269
Destination Port:	49199
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN EXE Download Request To Wordpress Folder Likely Malicious - Source IP: 192.168.2.22 - Destination IP: 115.186.131.16	
Timestamp:	192.168.2.22115.186.131.1649181802021697 02/01/23-22:33:20.436229
SID:	2021697
Source Port:	49181
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269491912841753 02/01/23-22:34:01.075251
SID:	2841753
Source Port:	6269
Destination Port:	49191
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 45.137.65.132 - Destination IP: 192.168.2.22	
Timestamp:	45.137.65.132192.168.2.226269491952841753 02/01/23-22:34:21.362666
SID:	2841753
Source Port:	6269
Destination Port:	49195
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Yara detected Nanocore RAT
- Multi AV Scanner detection for submitted file
- Multi AV Scanner detection for dropped file

Exploits

- Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)
- Office equation editor establishes network connection

Compliance

- Detected unpacking (overwrites its own PE header)

Software Vulnerabilities

Shellcode detected

Networking

Snort IDS alert for network traffic

Uses dynamic DNS services

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

HIPS / PFW / Operating System Protection Evasion

Maps a DLL or memory area into another process

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

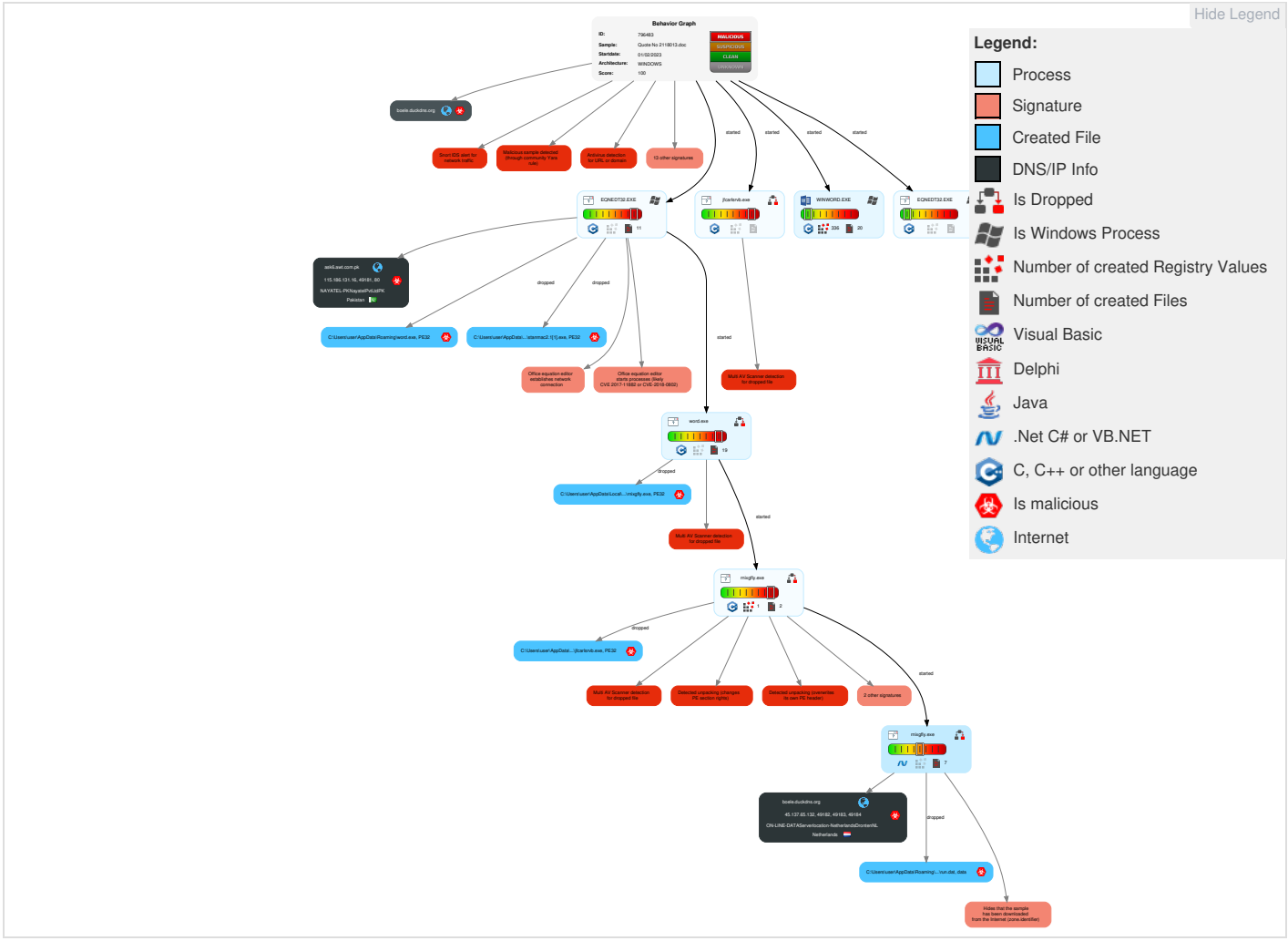
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 Access Token Manipulation	1 Disable or Modify Tools	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 3 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	1 Scripting	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 2 Native API	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Scripting	Security Account Manager	1 7 System Information Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	1 Non-Standard Port	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	2 3 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	3 Obfuscated Files or Information	NTDS	1 4 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Remote Access Software	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	2 Command and Scripting Interpreter	Network Logon Script	Network Logon Script	3 1 Software Packing	LSA Secrets	1 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	2 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Masquerading	Cached Domain Credentials	4 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	2 2 2 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	4 1 Virtualization/Sandbox Evasion	DCSync	1 Application Window Discovery	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 Access Token Manipulation	Proc Filesystem	1 Remote System Discovery	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 1 1 Process Injection	/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
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	1 Hidden Files and Directories	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols			Data Encrypted for Impact

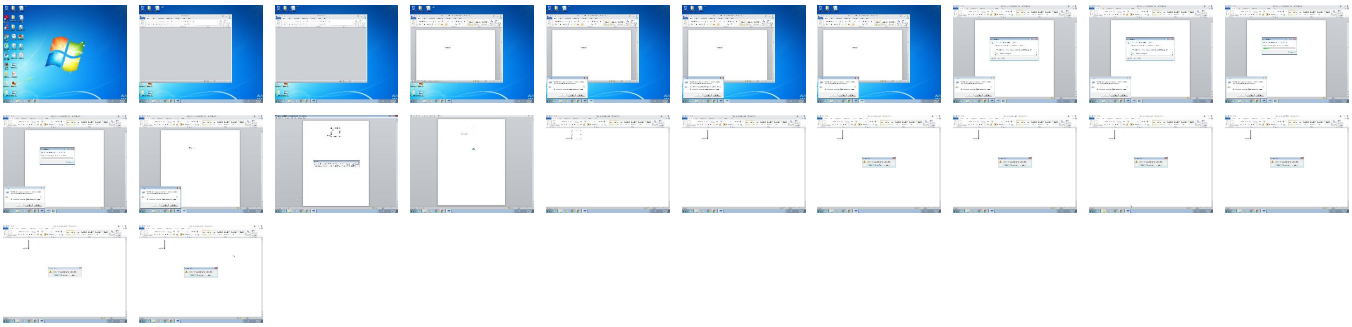
Behavior Graph

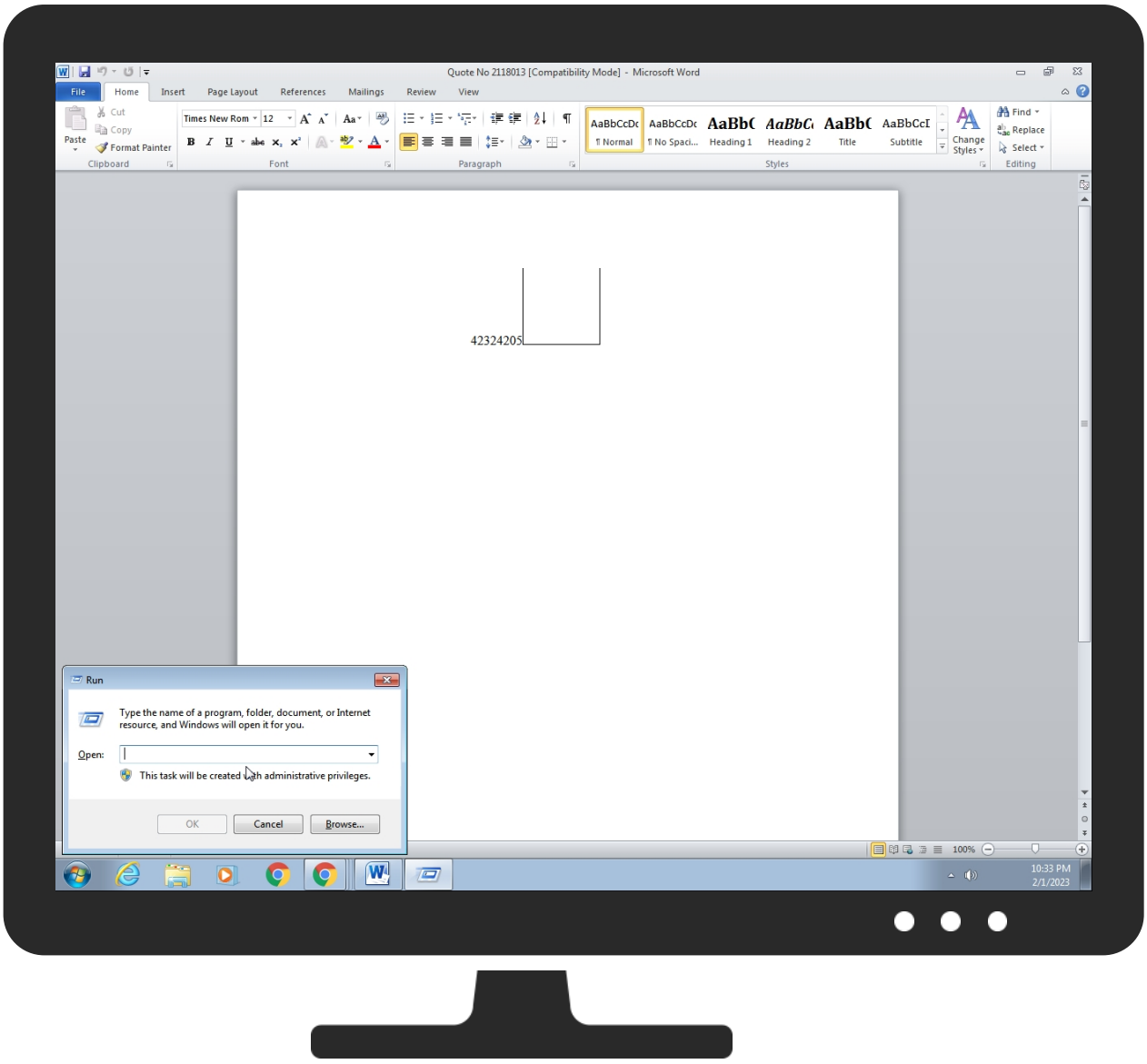


Screenshots

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
Quote No 2118013.doc	49%	ReversingLabs	Document-RTF.Exploit.CVE-2017-11882	
Quote No 2118013.doc	50%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\stanmac2.1[1].exe	65%	ReversingLabs	Win32.Trojan.Nemesis	
C:\Users\user\AppData\Local\Temp\rnixgfly.exe	41%	ReversingLabs	Win32.Trojan.InjectorX	
C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe	41%	ReversingLabs	Win32.Trojan.InjectorX	
C:\Users\user\AppData\Roaming\word.exe	65%	ReversingLabs	Win32.Trojan.Nemesis	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.rnixgfly.exe.1eb0000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
7.2.rnixgfly.exe.5000000.22.unpack	100%	Avira	TR/NanoCore.fadte		Download File
7.2.rnixgfly.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
5.2.word.exe.28407ec.1.unpack	100%	Avira	HEUR/AGEN.1230498		Download File
6.2.rnixgfly.exe.330000.0.unpack	100%	Avira	HEUR/AGEN.1230506		Download File

Domains

Source	Detection	Scanner	Label	Link
boele.duckdns.org	2%	Virustotal		Browse
ask6.awt.com.pk	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exeooC:	0%	Avira URL Cloud	safe	
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exeC	0%	Avira URL Cloud	safe	
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exeS	0%	Avira URL Cloud	safe	
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exe	100%	Avira URL Cloud	malware	
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exedoC:	0%	Avira URL Cloud	safe	
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exej	0%	Avira URL Cloud	safe	
boele.duckdns.org	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
boele.duckdns.org	45.137.65.132	true	true	• 2%, Virustotal, Browse	unknown
ask6.awt.com.pk	115.186.131.16	true	true	• 3%, Virustotal, Browse	unknown

Contacted URLs

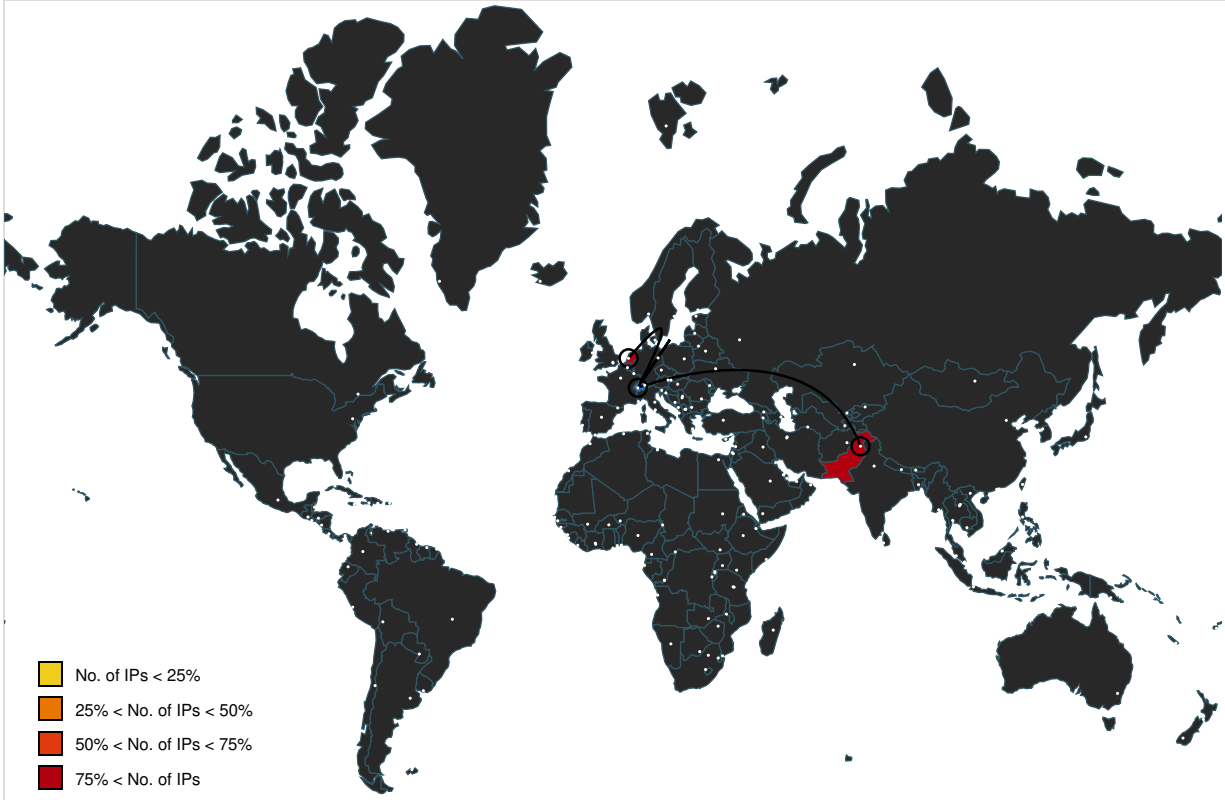
Name	Malicious	Antivirus Detection	Reputation
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exe	true	• Avira URL Cloud: malware	unknown
boele.duckdns.org	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exeC	EQNEDT32.EXE, 00000002.00000002.92006762 8.0000000000564000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exeS	EQNEDT32.EXE, 00000002.00000002.92006762 8.0000000000564000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exeooC:	EQNEDT32.EXE, 00000002.00000002.92006762 8.000000000056F000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	word.exe, 00000005.00000002.931066346.00 0000000040A000.00000004.00000001.0100000 0.00000004.sdmp, word.exe, 00000005.0000 0000.917193143.000000000040A000.00000008 .00000001.01000000.00000004.sdmp, stanma c2.1[1].exe.2.dr, word.exe.2.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	rnixgfly.exe, 00000007.00000002.11861508 13.0000000003523000.00000004.00000800.00 020000.00000000.sdmp, rnixgfly.exe, 0000 0007.00000003.1075179534.000000000367700 0.00000004.00000800.00020000.00000000.sdmp, rnixgfly.exe, 00000007.00000002.1188336607.000 0000006590000.00000004.08000000.00040000 .00000000.sdmp, rnixgfly.exe, 00000007.00000002.11 83458585.000000000227B000.00000004.00000 800.00020000.00000000.sdmp	false		high
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exedoC:	EQNEDT32.EXE, 00000002.00000003.91967038 8.0000000000636000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown
http://ask6.awt.com.pk/wordpress//wp-content/stanmac2.1.exej	EQNEDT32.EXE, 00000002.00000003.90743411 3.0000000000598000.00000004.00000020.000 20000.00000000.sdmp	true	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
115.186.131.16	ask6.awt.com.pk	Pakistan		23674	NAYATEL-PKNayatelPvtLtdPK	true
45.137.65.132	boele.duckdns.org	Netherlands		204601	ON-LINE-DATAServerlocation-NetherlandsDrontenNL	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	796483
Start date and time:	2023-02-01 22:32:21 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	14
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
Sample file name:	Quote No 2118013.doc
Detection:	MAL
Classification:	mal100.troj.expl.evad.winDOC@10/18@51/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 24.3% (good quality ratio 22.8%) • Quality average: 81.1% • Quality standard deviation: 28.6%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Attach to Office via COM • Active ActiveX Object • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 104.208.16.94, 104.208.16.93
- Excluded domains from analysis (whitelisted): onedsblobprdcus07.centralus.cloudapp.azure.com, watson.microsoft.com, legacywatson.trafficmanager.net, onedsblobprdcus16.centralus.cloudapp.azure.com
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:33:20	API Interceptor	332x Sleep call for process: EQNEDT32.EXE modified
22:33:29	API Interceptor	1871x Sleep call for process: rnixgfly.exe modified
22:33:30	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run ryhcwrfexidnfv C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe "C:\Users\user\AppData\Local\Temp\rnixgfly.exe" C:\Users\user\AppData\Lo
22:33:38	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run ryhcwrfexidnfv C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe "C:\Users\user\AppData\Local\Temp\rnixgfly.exe" C:\Users\user\AppData\Lo

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\stanmac2.1[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	430029
Entropy (8bit):	7.687199505367895
Encrypted:	false
SSDEEP:	6144:nYa603Pc/eEb9Ih4VB/Q3Eo1z/AMxf09Vi01XpSjROKeOSA3yPKN5nCugfzs0GFD:nYi0GEb9Z87jf+1wdPNiOh7gfzsh1
MD5:	D3E933B0AAB571BDC73355A106D657E0
SHA1:	EE600EACF16A1075FC8A28116A64F96403122D49
SHA-256:	51AB5D042DEE8DF90162A00A3307CF8D38D12BC54B7DC07C756996AA0F6B3804
SHA-512:	DB4CF8C673E8FA839AD9AF7EDD61F00D57D24BA68955E97E4ACC2F0A3046C4AA91A63C2A0C3803DE3276B6CB7BA1F27F66732E2A023C0D0F484F4B457FC9F4 2C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 65%
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...*.....@6.....@.....@..... .....text...vf.....h..... ..`.rdata.....l.....@..@.data...x.....@....ndata.....rsrc.....@..@..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{0A4B3911-FEFD-4AA5-A41A-6550C2F96D9E}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	376832
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	FC0418AFEBA826A80D97EEF93EA74430
SHA1:	64DF9DBDB5043AA6EB622B01AEC52577634BE2C2
SHA-256:	ECE761FC8648D152E7F761E8992079946868B88F75AD66122D822D5CB2DF316E
SHA-512:	368A1C59BE8F79F3CF021F8810847F96BE147AB6EC1B5F92801E2F329CD453B260EFF8B0DE6719A1A93BEADABF8603F2A9854EA358929DF22EF57C6582761951
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{D6D5F209-138C-443D-8A21-E23B722EB3AB}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped

Size (bytes):	1024
Entropy (8bit):	0.9176185571932136
Encrypted:	false
SSDEEP:	6:gzv+lwwNgREqAWlgFJkSDlll8vlwT3FwQFrB:iv+ldk5uFJn7uvqLKQZB
MD5:	6AF3F880A6F0E2839A2E6CF5843D3137
SHA1:	342960F498CCE021C1865634AC9A0BE84F4783FE
SHA-256:	DFF79D49203CA4D94620A345AABAD93563F76E69CBA99F6C5282299A8F1FB926
SHA-512:	11B32FF4857D06B5CD598A08ABCEB6280A19559AF0ACD85846A892527AB493E6EA5477BCD2805765624417DBF6A9F2849ECF186154E3F2F7018A2FB9FB15C87(
Malicious:	false
Preview:	.....4.2.3.2.4.2.0.5.=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ....".... .....j....CJ..OJ..QJ..U..^J..aJ.. .j0g.g...CJ..OJ..QJ..U..^J..aJ.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{E00A286F-D9E2-457B-B119-BAD556F2C91B}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28E A4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\nsl3E1A.tmp

Process:	C:\Users\user\AppData\Roaming\word.exe
File Type:	data
Category:	dropped
Size (bytes):	406476
Entropy (8bit):	7.760217782520545
Encrypted:	false
SSDEEP:	12288:DfIs4bcdUHKgcuzRlCDlNXhJGjvwDjpzxTSmFTo:DfIhcdUD1lC7hJGs5xTjBo
MD5:	306A577A34A568DC94A31C8EB371E05A
SHA1:	5EA8978456D1F1198C9C806F9435DA09EA943555
SHA-256:	50F3AC3A1EBC8EC50D101E815DDB00A1DE7284D85C5502E7569C3BC7BCF91F25
SHA-512:	0E9A2A2228694DC61F206BD8897C645FF8E76B635ECC22AF5262C2196E13D32CBDEDFF6BDF26637BD3BF8D387C6556A78781828E4390B2C29973040B17A376B
Malicious:	false
Preview:	&6.....y...0'.....@5.....6..... .....G.....j.....9..... ....

C:\Users\user\AppData\Local\Temp\rnixgfly.exe

Process:	C:\Users\user\AppData\Roaming\word.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	76800
Entropy (8bit):	6.349678040473841
Encrypted:	false
SSDEEP:	1536:v/9cl7eE+7q3xJ6qI8ZZ9kmQFo4EFFWD3gjn5LIPU4l3:v/9clWcxTZ3km34EFkOX4l3
MD5:	C1DC97853E14C21B463C6E95B21C300C
SHA1:	78ADBB8A1EFCB4F0AB5BEBA8A3CF70E5074BE945
SHA-256:	F18C6867F028E0E31A939FDB580762F57DCD11BB25B11E632EE22F21203DCC31

SHA-512:	04DFC132DBC5D31EBEA2E8453F065E2FCB67224F60A0EB0F53C27CBA6A36208A915E14B8E877F92C5FBA5C583580EBF759BFC650D7B95A526E4703A71F700A2B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Oe8%..Vv..Vv..Vvdr.v+.Vvdr.v..Vv.|.v..Vv..Wv..Vvdr.v|.Vvdr.v..VvRich..Vv.....PE..L.....c.....v.....3.....@.....#.....text...J..... ..`.rdata...1.....2.....@..@.data...B...@.....@..... .....

C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt

Process:	C:\Users\user\AppData\Roaming\word.exe
File Type:	data
Category:	dropped
Size (bytes):	7840
Entropy (8bit):	7.191226445255042
Encrypted:	false
SSDEEP:	192:darcitQvArWiPvECb9l5E3JHuQOoLHqGDcfumovUX7fN+:uCYrNPvEEzOjnKRmdsLN+
MD5:	E3C9D191E461DB735E4FDF1AC0FD72A5
SHA1:	0E8F30B10F46933786D4525F59D4ABEA09D519FC
SHA-256:	20838738B10F16E37211678286DBE6E5561E0057770344D5C9BF9F6865FC217D
SHA-512:	C04EE58FFC5ACCEFBE16F5F36281348E1D536E8E47105CF7A70D67FE93ED4A517FE164F960EFFF45A43EE40D5453A63D176E8FE44928D12AD469A0C043A935A2
Malicious:	false
Preview:	.705m..f.F<...05o.:.....?v>.3.3.<.....M.knl.02a..c.E<...42c. .....4.D63.6.3.?.....E.gni.53P..805.p8.q?.2.8.u .a..beabo.H0..v..v.@3.`..i/7.p.6.t(2..g.}.u<..G-.0.3.h.f....w8L$.m.r .D;F...okc..m.;4.q.?.<@.4.0...m..u<f...@%.`4..D'd.O$..A5..=..<r..4M.knl.82a..Q..401ec.t4.M4...D;.D..d580..E9....E....3.u.mje.18e..`W..480.x<.p=.4.4.p-P..6.c.!....D%.|.eX. ....+..t..0....e.a..`beP..580.p=.t>.8.5.p,XE..Md.....M9..e...@4.....F1..u.|c.....Lq.}<...v<+480.}<;.&<.>..r.^.q8F0....q.^.q8F0...^..M...3uc.....}<F...kloe.=8e....aboZf`Z\V.v...`ZY aZCV.v.j^YV.}.lZAU.w.`Z\^.q.iY.T.}.m^.q.[WlT.}....i.W.y.R.}.^.y.W.q.....XW..Mc.....\7!.K.y.a..`.....Z...Jo.....\GB.Gg.u.....X.B.Kg.v.....Pp..Nd.w.....\...Ke.}.....Y...Ko.p... ...G8.u....0<..480fP.401Y7a^?X580..D;.g.....A4...Tgn.`...G.X0P0.80..3cg.a.p0..D.`...igen.a..@.b.e.kX.013^3gR7]804p.F8.a.c..q.ad.G<n.`..D2..qb.e...knj..o.00`...)ecXg`Z]^.q .iYXk^OV.}.lZPU.w.`ZE^.q.iY]T.}.mR.R.t.lT.}._\hR.t...R.}.^.y.W.y.R.u.....ZR..Jo....\5$.O

C:\Users\user\AppData\Local\Temp\vvnwaf.f

Process:	C:\Users\user\AppData\Roaming\word.exe
File Type:	data
Category:	dropped
Size (bytes):	307958
Entropy (8bit):	7.98837190566036
Encrypted:	false
SSDEEP:	6144:hApS0PxPJG0RbcXNuGiHKgagwuzHEElCDlN5yObFhM4Gj0cwzRFE:hfIs4bcdUHKgcuzRlCDlNXhJGjvwDE
MD5:	FC0382D6DBF66C328188C64CACD86ED6
SHA1:	F7AF5088065FD1F9B66D8F4EE4041E3B8430CC33
SHA-256:	60C585E63B9378D1ED35E059B6BC6CC362129A4BFD40F70B0037724C1540AA54
SHA-512:	300D0BB1FBA8E4CE455C9B0AF121A247FA94A3DDE5D37339FC6CCA1DCB52D568C6EAD0CEA6484A26C574AE03059ADCF2FF24BC4C114ADF54EE10DA1874664B2A
Malicious:	false
Preview:	Cs...w.W7.3.=Q.....4....L".O..$J{..{.....#..+.E..4...Y...6.).P.8...^.....Y..M..m.v.4AI..*.p.8..i.M5.Z-u..q..".G.>..wq...D...v.!W.bX..+..f.....>#uRS>.~3.$Oty.}.WeL.].t..o...Y .F.S.F..G..k...g...."...S..S....$.....4h.....h.."...'.C.q..i.w..:.3....1...4....L".O.0.q.r.....>#..1.E..4..~.@.X).7u..\|1....]..k.....p..A.z.1.KAu...y{aS4.P....M.U.G.T>..R..e.]ho.[....{.7.N ..PMY}_.s.....U@.....d>.8...>5o....e..lh.V.v.%...'..Os....?./..s.?.=.b4.KLc<.....n."QX.Cn."...'.C..../.w...3ZxQ..].....L".O..$J{.C{..Sj.g.R..{.#....E.4...Y....X)i7u..|1.....$`.....E .....zU1.!..`..y{wS4.P.K.MP..B.>....e.\.h.*....r{...N+..MY}_.B..q..U@.....d>.8..a..5y....e..lh.V.v.%...'..Os....Du\|..s.?.=.b4.KLcg.....n."QX.Cn."...'.C.q..i.w..7.3Z`Q.....4.. ..L".O..$J{..{.....#..+.E..4..~Y....X)i7u..|1.....]..k.....A.z.1.!Au`..y{wS4.P...M.U.G.>..R..e.]h.2....{...N+..MY}_.s.....U@.....d>.8..a..5y....e..lh.V.v.%...'..Os....Du|..s.?.=.b4. KLcg.....

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat

Process:	C:\Users\user\AppData\Local\Temp\rnixgfly.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:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35(A5
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\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat

Process:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	2.75
Encrypted:	false
SSDEEP:	3:USn:t
MD5:	5873CC731E0B0ED8A30A7A1352D9CD3F
SHA1:	D549B27BA58594AA768399E7376AA1C893C6B6C3
SHA-256:	216CD4C262E265C2DE1CC1DA77CC3802C40F96C58833DFD353B01FD5BB605D41
SHA-512:	2E72F4F62F0D58CA1014AFBA4A8DDA34C58AE4D5CF6F8C47BA18EF0EA0F155956A579118E6344F84734D573348C7DA55C8004E98F13ADD27A6AC7E035F3F1D 0
Malicious:	**true**
Preview:	..~f...H

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bin

Process:	C:\Users\user\AppData\Local\Temp\rnixgfly.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:	DD44C2D24D4E3A0F0B988AD3D04683B5CB128298043134649BBE33B2512CE0C9B1A8E7D893B9F66FBBCDD901E2B0646C4533FB6C0C8C4AFCB95A0EFB95D44 F8
Malicious:	false
Preview:	9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat

Process:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92 6
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...I.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Quote No 2118013.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE

File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Mar 8 15:45:59 2022, mtime=Tue Mar 8 15:45:59 2022, atime=Thu Feb 2 05:33:18 2023, length=715212, window=hide
Category:	dropped
Size (bytes):	1044
Entropy (8bit):	4.53236694763466
Encrypted:	false
SSDEEP:	12:87m6wmjut6hgXg/XAlCPCHaXMBzB/wpvX+WHiUHcfCi00icvbIZrxyDtZ3YilMMr:87m69d/XT898vUU2l8eEZsDv3q3u7D
MD5:	6A4BF7EE3A97A685B44C697EAD9E4037
SHA1:	668EC24F8888FF6EB4FB8BA25A42C85338340759
SHA-256:	2E7170349DFB208ECBF71AFD2832D173DE98948CA503465F532D83855A05D7B4
SHA-512:	599615309C040B449D0A492AD971E4FBA8472DAD64EB59F42F7A6C6831442A305342C8241FD97771F5A3125A9100E0EB054A789F7F28B23F03601FDEA5D2D17C
Malicious:	false
Preview:	L.....F.... .....3.....3...h.<.6.....P.O. ..i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....hT...Desktop.d.....QK.XhT.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....r.2.....BV*4 .QUOTEN~1.DOC..V.....hT..hT..*...r.....'.....Q.u.o.t.e. .N.o. .2.1.1.8.0.1.3...d.o.c.....~.....-...8...[.....?J.....C:\Users\..#.....\\414408\Users.user\Desktop\Quote No 2118013.doc.+.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.Q.u.o.t.e. .N.o. .2.1.1.8.0.1.3...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....414408.....D_....3N...W...9G..N....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Generic INItialization configuration [doc]
Category:	dropped
Size (bytes):	83
Entropy (8bit):	4.678145577230597
Encrypted:	false
SSDEEP:	3:bDuMJlsQKjPYmX12PYv:bC7P+PC
MD5:	9B2125059B9276B37AA0F5998C115864
SHA1:	1CF2AF4ACC610B61281998859833DFCE3043754C
SHA-256:	09F3DA1B41D2A803C094B5BB35D9008EE658F97E70BC2CD73F51BB5FD23864AD
SHA-512:	3B353DDD0EC8BD6F51323DE9C75CCFD9216577E1CC4B2C25BE278DFAECD7374100A7E4C1949FB083EDD62AA791C1C342D28B56E88F8A78A21381127CE5F40DE
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Quote No 2118013.LNK=0..[doc]..Quote No 2118013.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe

Process:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	76800
Entropy (8bit):	6.349678040473841
Encrypted:	false
SSDEEP:	1536:v/9cl7eE+7q3xJ6qI8ZZ9kmQFo4EFFWD3gjn5LIPU4l3:v/9clWcxTZ3km34EFkOX4l3
MD5:	C1DC97853E14C21B463C6E95B21C300C
SHA1:	78ADBB8A1EFCB4F0AB5BEBA8A3CF70E5074BE945
SHA-256:	F18C6867F028E0E31A939FDB580762F57DCD11BB25B11E632EE22F21203DCC31

SHA-512:	04DFC132DBC5D31EBEA2E8453F065E2FCB67224F60A0EB0F53C27CBA6A36208A915E14B8E877F92C5FBA5C583580EBF759BFC650D7B95A526E4703A71F700A2B
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 41%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Oe8%..Vv..Vv..Vvdr.v+.Vvdr.v..Vv.|.v..Vv..Wv..Vvdr.v|.Vvdr.v..VvRich..Vv.....PE..L.....c.....v.....3.....@.....#.....text...J..... ..`.rdata...1.....2.....@..@.data...B...@.....@.....

C:\Users\user\AppData\Roaming\word.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	430029
Entropy (8bit):	7.687199505367895
Encrypted:	false
SSDEEP:	6144:nYa603Pc/eEb9Ih4VB/Q3Eo1z/AMxf09Vi01XpSjROKeOSA3yPKN5nCugfzs0GFD:nYi0GEb9Z87jf+1wdPNiOh7gfzsh1
MD5:	D3E933B0AAB571BDC73355A106D657E0
SHA1:	EE600EACF16A1075FC8A28116A64F96403122D49
SHA-256:	51AB5D042DEE8DF90162A00A3307CF8D38D12BC54B7DC07C756996AA0F6B3804
SHA-512:	DB4CF8C673E8FA839AD9AF7EDD61F00D57D24BA68955E97E4ACC2F0A3046C4AA91A63C2A0C3803DE3276B6CB7BA1F27F66732E2A023C0D0F484F4B457FC9F2C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 65%
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...*.....@6.....@.....@.....text...vf.....h..... ..`.rdata.....l.....@..@.data...x.....@....ndata.....rsrc.....@..@.....

C:\Users\user\Desktop\~$ote No 2118013.doc

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyHH/cgQfmW+eMdln:vdsCkWtUb+8ll
MD5:	D9C8F93ADB8834E5883B5A8AAAC0D8D9
SHA1:	23684CCAA587C442181A92E722E15A685B2407B1
SHA-256:	116394FEAB201D23FD7A4D7F6B10669A4CBCE69AF3575D9C1E13E735D512FA11
SHA-512:	7742E1AC50ACB3B794905CFAE973FDBF16560A7B580B5CD6F27FEFE1CB3EF4AEC2538963535493DCC25F8F114E8708050EDF5F7D3D146DF47DA4B958F052655
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....15.....25.....@35.....35.....z.....p45.....x...

Static File Info

General

File type:	Rich Text Format data, version 1
Entropy (8bit):	4.002054496788941
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Quote No 2118013.doc
File size:	715212
MD5:	342550e9ccd167df75606545a53e9b0a
SHA1:	30f28411b298aeda401364af8f27f164d634a567
SHA256:	9ab75f3c60adc58693a916cac8ec6dbe53f32d5355ab5db8587693c0426be40b
SHA512:	5ac761ba399edc52f1b0c5b850b9bea81c575e872dcd2add2a67a70e9eee7d4a7d07b0c7afcbec9f1fb80f8019803f0ab97883232e479dcfeeb3fe18fe7ceb1c

SSDEEP:	12288:IK33yN0sc7FqjxRdCgaW6rMgsy7Q20LlUHnql7zaimJfl3Rcbws3wIELpMG:IR0sca57acRr2olO9blhcbwDG
TLSH:	3DE4BFB876047DD62A7F576BDA96ADD803B62B238ACBA4CD806477C30563375FE02C05
File Content Preview:	{\rtf1.....{*\wzAppletArg991826410 \+}.{\142324205\object54623845\objlink65003839\objw2472\objh3625{*\objdata252362{*\aoutl206902499 \bin0000000\.194611485146808977}.{*\stylenames80723639 \bin00000\.30333813198601957}.1cf9677e020000000b00000065515

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000075h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2245.137.65.132492006269281676602/01/23-22:34:43.189770	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49200	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491926269281676602/01/23-22:34:05.557258	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49192	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491886269202501902/01/23-22:33:46.711822	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49188	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.226269492082841753 02/01/23-22:35:24.322607	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49208	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.132492036269281676602/01/23-22:34:58.588930	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49203	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132492066269202501902/01/23-22:35:14.040549	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49206	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491856269281676602/01/23-22:33:42.424345	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49185	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491906269281671802/01/23-22:33:56.804784	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49190	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132492016269202501902/01/23-22:34:48.135847	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49201	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132492016269281671802/01/23-22:34:48.213161	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49201	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491956269281676602/01/23-22:34:21.457259	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49195	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491936269202501902/01/23-22:34:10.437260	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49193	6269	192.168.2.22	45.137.65.132

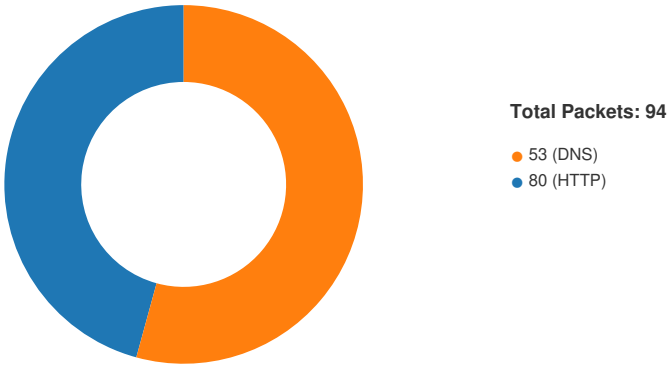
Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2245.137.65.132491836269202501902/01/23-22:33:33.655639	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49183	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132492086269281676602/01/23-22:35:24.406415	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49208	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491826269281676602/01/23-22:33:29.150304	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49182	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132492056269281676602/01/23-22:35:09.135573	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49205	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491846269281676602/01/23-22:33:38.036128	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49184	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491946269281676602/01/23-22:34:17.104190	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49194	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.226269491832841753 02/01/23-22:33:33.694801	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49183	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.132491926269202501902/01/23-22:34:05.362301	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49192	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491996269202501902/01/23-22:34:38.766002	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49199	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132492046269202501902/01/23-22:35:03.284314	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49204	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.226269491982841753 02/01/23-22:34:34.472656	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49198	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.132491906269202501902/01/23-22:33:56.681631	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49190	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491936269281676602/01/23-22:34:11.683759	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49193	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.226269491892841753 02/01/23-22:33:52.332924	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49189	45.137.65.132	192.168.2.22
45.137.65.132192.168.2.226269492002841753 02/01/23-22:34:43.093025	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49200	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.132491896269202501902/01/23-22:33:52.298886	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49189	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.132491986269202501902/01/23-22:34:34.436858	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49198	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.226269491852841753 02/01/23-22:33:42.356276	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49185	45.137.65.132	192.168.2.22
45.137.65.132192.168.2.226269491962841753 02/01/23-22:34:25.705442	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49196	45.137.65.132	192.168.2.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.137.65.132192.168.2.226269491902841753 02/01/23-22:33:56.719131	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49190	45.137.65.132	192.168.2.22
45.137.65.132192.168.2.226269491922841753 02/01/23-22:34:05.398117	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49192	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.1324920362692025019 02/01/23-22:34:58.374868	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49203	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324920662692816766 02/01/23-22:35:14.483677	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49206	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324918962692816766 02/01/23-22:33:52.436607	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49189	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324919162692025019 02/01/23-22:34:01.037424	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49191	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324919662692816766 02/01/23-22:34:25.729294	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49196	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324919962692816766 02/01/23-22:34:38.834547	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49199	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324919462692025019 02/01/23-22:34:16.062227	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49194	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324918462692025019 02/01/23-22:33:37.918139	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49184	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324918362692816766 02/01/23-22:33:33.792254	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49183	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324920262692025019 02/01/23-22:34:53.384126	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49202	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324920862692025019 02/01/23-22:35:24.288274	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49208	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324920762692816766 02/01/23-22:35:20.080067	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49207	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324919762692025019 02/01/23-22:34:30.147504	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49197	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.226269491932810290 02/01/23-22:34:11.805752	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	6269	49193	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.1324920562692025019 02/01/23-22:35:08.089961	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49205	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324920462692816766 02/01/23-22:35:03.782867	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49204	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.1324920062692025019 02/01/23-22:34:43.058807	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49200	6269	192.168.2.22	45.137.65.132

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2245.137.65.13 24920762692025019 02/01/23- 22:35:18.957271	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49207	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.13 24921062692025019 02/01/23- 22:35:28.658958	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49210	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.2 26269491842841753 02/01/23- 22:33:37.953540	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49184	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.13 24919662692025019 02/01/23- 22:34:25.668610	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49196	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.13 24919762692816766 02/01/23- 22:34:30.191917	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49197	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.13 24919162692816766 02/01/23- 22:34:01.259922	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49191	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.13 24920162692816766 02/01/23- 22:34:48.556940	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49201	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.13 24918562692025019 02/01/23- 22:33:42.320152	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49185	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.2 26269492102841753 02/01/23- 22:35:28.695632	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49210	45.137.65.132	192.168.2.22
45.137.65.132192.168.2.2 26269491882841753 02/01/23- 22:33:46.748199	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49188	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.13 24919562692025019 02/01/23- 22:34:21.323516	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49195	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.13 24919862692816766 02/01/23- 22:34:34.560423	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49198	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.2 26269492032841753 02/01/23- 22:34:58.443751	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49203	45.137.65.132	192.168.2.22
192.168.2.2245.137.65.13 24920262692816766 02/01/23- 22:34:53.943308	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49202	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.13 24919062692816766 02/01/23- 22:33:56.804784	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49190	6269	192.168.2.22	45.137.65.132
192.168.2.2245.137.65.13 24918862692816766 02/01/23- 22:33:46.773305	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49188	6269	192.168.2.22	45.137.65.132
45.137.65.132192.168.2.2 26269491972841753 02/01/23- 22:34:30.181373	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49197	45.137.65.132	192.168.2.22
45.137.65.132192.168.2.2 26269491992841753 02/01/23- 22:34:38.800055	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49199	45.137.65.132	192.168.2.22
192.168.2.22115.186.131. 1649181802021697 02/01/23- 22:33:20.436229	TCP	2021697	ET TROJAN EXE Download Request To Wordpress Folder Likely Malicious	49181	80	192.168.2.22	115.186.131.16

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
45.137.65.132192.168.2.226269491912841753 02/01/23-22:34:01.075251	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49191	45.137.65.132	192.168.2.22
45.137.65.132192.168.2.226269491952841753 02/01/23-22:34:21.362666	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	6269	49195	45.137.65.132	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 22:33:20.287925005 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.435137987 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.435421944 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.436228991 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.588872910 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.588910103 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.588929892 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.588951111 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.589066982 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.590477943 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.737171888 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.737266064 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.737320900 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.737377882 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.737392902 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.737440109 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.737452030 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.737497091 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.737499952 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.737546921 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.737566948 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.737595081 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.737597942 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.737641096 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.737643003 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.737797022 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885023117 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885067940 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885096073 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885118008 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885138035 CET	80	49181	115.186.131.16	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 22:33:20.885159016 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885181904 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885183096 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885209084 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885209084 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885236025 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885246038 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885265112 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885284901 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885292053 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885317087 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885318995 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885345936 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885346889 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885370970 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885380983 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885401011 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885406017 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885428905 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:20.885438919 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885463953 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.885474920 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:20.886101007 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032495022 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032536983 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032557964 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032581091 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032603025 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032622099 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032641888 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032661915 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032660007 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032681942 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032696009 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032702923 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032706022 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032722950 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032727957 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032742977 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032751083 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032764912 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032778978 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032784939 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032804012 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032808065 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032824039 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032829046 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032844067 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032851934 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032865047 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032875061 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032885075 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032898903 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032905102 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032922983 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032924891 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032946110 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032947063 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032965899 CET	80	49181	115.186.131.16	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 22:33:21.032967091 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.032984972 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.032989025 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.033005953 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.033011913 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.033026934 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.033034086 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.033046007 CET	80	49181	115.186.131.16	192.168.2.22
Feb 1, 2023 22:33:21.033065081 CET	49181	80	192.168.2.22	115.186.131.16
Feb 1, 2023 22:33:21.033066988 CET	80	49181	115.186.131.16	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 22:33:20.247306108 CET	59915	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:20.267151117 CET	53	59915	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:28.616257906 CET	54408	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:28.725162029 CET	53	54408	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:28.730607986 CET	54408	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:28.840111017 CET	53	54408	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:28.840572119 CET	54408	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:28.859941959 CET	53	54408	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:33.292978048 CET	50108	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:33.401619911 CET	53	50108	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:33.402273893 CET	50108	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:33.508759022 CET	53	50108	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:33.509409904 CET	50108	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:33.529383898 CET	53	50108	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:37.866092920 CET	54723	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:37.883954048 CET	53	54723	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:42.143568993 CET	58062	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:42.250889063 CET	53	58062	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:42.251219988 CET	58062	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:42.268738985 CET	53	58062	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:42.269176006 CET	58062	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:42.286823034 CET	53	58062	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:46.530886889 CET	56020	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:46.639110088 CET	53	56020	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:46.639703989 CET	56020	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:46.658994913 CET	53	56020	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:46.659481049 CET	56020	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:46.678929090 CET	53	56020	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:51.231370926 CET	51663	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:51.339474916 CET	53	51663	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:51.514202118 CET	51663	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:51.534178972 CET	53	51663	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:52.112663031 CET	51663	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:52.221016884 CET	53	51663	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:52.245512009 CET	51663	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:52.265419960 CET	53	51663	8.8.8.8	192.168.2.22
Feb 1, 2023 22:33:56.630445004 CET	51020	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:33:56.648233891 CET	53	51020	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:00.988929033 CET	60622	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:01.006854057 CET	53	60622	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:05.312952042 CET	53160	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:05.330677986 CET	53	53160	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:10.314642906 CET	64948	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:10.332300901 CET	53	64948	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:10.332724094 CET	64948	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 1, 2023 22:34:10.350460052 CET	53	64948	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:16.003199100 CET	64281	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:16.020915031 CET	53	64281	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:21.274357080 CET	63396	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:21.292143106 CET	53	63396	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:25.615905046 CET	60506	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:25.636167049 CET	53	60506	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:29.969865084 CET	52585	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:30.076360941 CET	53	52585	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:30.076874018 CET	52585	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:30.094160080 CET	53	52585	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:30.094882011 CET	52585	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:30.114598036 CET	53	52585	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:34.385663986 CET	52129	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:34.404181957 CET	53	52129	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:38.716540098 CET	57078	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:38.734345913 CET	53	57078	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:43.009109020 CET	52276	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:43.026751995 CET	53	52276	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:47.375459909 CET	53057	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:47.482248068 CET	53	53057	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:47.484711885 CET	53057	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:47.592971087 CET	53	53057	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:47.595331907 CET	53057	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:47.612920046 CET	53	53057	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:47.613362074 CET	53057	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:47.630901098 CET	53	53057	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:52.665399075 CET	64788	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:52.772857904 CET	53	64788	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:52.776482105 CET	64788	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:52.884701967 CET	53	64788	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:52.885283947 CET	64788	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:52.902323961 CET	53	64788	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:58.198164940 CET	63728	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:58.304527998 CET	53	63728	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:58.305036068 CET	63728	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:58.322787046 CET	53	63728	8.8.8.8	192.168.2.22
Feb 1, 2023 22:34:58.323455095 CET	63728	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:34:58.341437101 CET	53	63728	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:02.714750051 CET	56509	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:02.732624054 CET	53	56509	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:07.928937912 CET	51925	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:08.037184000 CET	53	51925	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:08.037664890 CET	51925	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:08.057095051 CET	53	51925	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:13.263467073 CET	62474	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:13.372343063 CET	53	62474	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:13.372951031 CET	62474	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:13.390119076 CET	53	62474	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:13.390666962 CET	62474	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:13.408463001 CET	53	62474	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:18.708826065 CET	51840	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:18.726483107 CET	53	51840	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:24.237289906 CET	51454	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:24.255112886 CET	53	51454	8.8.8.8	192.168.2.22
Feb 1, 2023 22:35:28.605782032 CET	63972	53	192.168.2.22	8.8.8.8
Feb 1, 2023 22:35:28.625910997 CET	53	63972	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 22:33:20.247306108 CET	192.168.2.22	8.8.8.8	0x5c77	Standard query (0)	ask6.awt.com.pk	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:28.616257906 CET	192.168.2.22	8.8.8.8	0x5ff7	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:28.730607986 CET	192.168.2.22	8.8.8.8	0x5ff7	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:28.840572119 CET	192.168.2.22	8.8.8.8	0x5ff7	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:33.292978048 CET	192.168.2.22	8.8.8.8	0xf1f0	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:33.402273893 CET	192.168.2.22	8.8.8.8	0xf1f0	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:33.509409904 CET	192.168.2.22	8.8.8.8	0xf1f0	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:37.866092920 CET	192.168.2.22	8.8.8.8	0xcf73	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:42.143568993 CET	192.168.2.22	8.8.8.8	0x7151	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:42.251219988 CET	192.168.2.22	8.8.8.8	0x7151	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:42.269176006 CET	192.168.2.22	8.8.8.8	0x7151	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:46.530886889 CET	192.168.2.22	8.8.8.8	0x5624	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:46.639703989 CET	192.168.2.22	8.8.8.8	0x5624	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:46.659481049 CET	192.168.2.22	8.8.8.8	0x5624	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:51.231370926 CET	192.168.2.22	8.8.8.8	0x3474	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:51.514202118 CET	192.168.2.22	8.8.8.8	0x3474	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:52.112663031 CET	192.168.2.22	8.8.8.8	0x3474	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:52.245512009 CET	192.168.2.22	8.8.8.8	0x3474	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:56.630445004 CET	192.168.2.22	8.8.8.8	0xa3f3	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:00.988929033 CET	192.168.2.22	8.8.8.8	0x9bf2	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:05.312952042 CET	192.168.2.22	8.8.8.8	0x9788	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:10.314642906 CET	192.168.2.22	8.8.8.8	0x40bd	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:10.332724094 CET	192.168.2.22	8.8.8.8	0x40bd	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:16.003199100 CET	192.168.2.22	8.8.8.8	0x3956	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:21.274357080 CET	192.168.2.22	8.8.8.8	0xedae	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:25.615905046 CET	192.168.2.22	8.8.8.8	0xda4c	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:29.969865084 CET	192.168.2.22	8.8.8.8	0xe283	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:30.076874018 CET	192.168.2.22	8.8.8.8	0xe283	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:30.094882011 CET	192.168.2.22	8.8.8.8	0xe283	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:34.385663986 CET	192.168.2.22	8.8.8.8	0xe3ae	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:38.716540098 CET	192.168.2.22	8.8.8.8	0xe571	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:43.009109020 CET	192.168.2.22	8.8.8.8	0x6377	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:47.375459909 CET	192.168.2.22	8.8.8.8	0x785	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:47.484711885 CET	192.168.2.22	8.8.8.8	0x785	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 1, 2023 22:34:47.595331907 CET	192.168.2.22	8.8.8.8	0x785	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:47.613362074 CET	192.168.2.22	8.8.8.8	0x785	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:52.665399075 CET	192.168.2.22	8.8.8.8	0x3c29	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:52.776482105 CET	192.168.2.22	8.8.8.8	0x3c29	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:52.885283947 CET	192.168.2.22	8.8.8.8	0x3c29	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:58.198164940 CET	192.168.2.22	8.8.8.8	0xaee9	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:58.305036068 CET	192.168.2.22	8.8.8.8	0xaee9	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:58.323455095 CET	192.168.2.22	8.8.8.8	0xaee9	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:02.714750051 CET	192.168.2.22	8.8.8.8	0xde9a	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:07.928937912 CET	192.168.2.22	8.8.8.8	0x6b9	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:08.037664890 CET	192.168.2.22	8.8.8.8	0x6b9	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:13.263467073 CET	192.168.2.22	8.8.8.8	0x3c9d	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:13.372951031 CET	192.168.2.22	8.8.8.8	0x3c9d	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:13.390666962 CET	192.168.2.22	8.8.8.8	0x3c9d	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:18.708826065 CET	192.168.2.22	8.8.8.8	0x617e	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:24.237289906 CET	192.168.2.22	8.8.8.8	0x7e09	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:28.605782032 CET	192.168.2.22	8.8.8.8	0x3b94	Standard query (0)	boele.duckdns.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 22:33:20.267151117 CET	8.8.8.8	192.168.2.22	0x5c77	No error (0)	ask6.awt.com.pk		115.186.131.16	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:28.725162029 CET	8.8.8.8	192.168.2.22	0x5ff7	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:28.840111017 CET	8.8.8.8	192.168.2.22	0x5ff7	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:28.859941959 CET	8.8.8.8	192.168.2.22	0x5ff7	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:33.401619911 CET	8.8.8.8	192.168.2.22	0xf1f0	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:33.508759022 CET	8.8.8.8	192.168.2.22	0xf1f0	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:33.529383898 CET	8.8.8.8	192.168.2.22	0xf1f0	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:37.883954048 CET	8.8.8.8	192.168.2.22	0xcf73	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:42.250889063 CET	8.8.8.8	192.168.2.22	0x7151	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:42.268738985 CET	8.8.8.8	192.168.2.22	0x7151	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:42.286823034 CET	8.8.8.8	192.168.2.22	0x7151	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 22:33:46.639110088 CET	8.8.8.8	192.168.2.22	0x5624	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:46.658994913 CET	8.8.8.8	192.168.2.22	0x5624	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:46.678929090 CET	8.8.8.8	192.168.2.22	0x5624	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:51.339474916 CET	8.8.8.8	192.168.2.22	0x3474	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:51.534178972 CET	8.8.8.8	192.168.2.22	0x3474	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:52.221016884 CET	8.8.8.8	192.168.2.22	0x3474	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:52.265419960 CET	8.8.8.8	192.168.2.22	0x3474	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:33:56.648233891 CET	8.8.8.8	192.168.2.22	0xa3f3	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:01.006854057 CET	8.8.8.8	192.168.2.22	0x9bf2	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:05.330677986 CET	8.8.8.8	192.168.2.22	0x9788	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:10.332300901 CET	8.8.8.8	192.168.2.22	0x40bd	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:10.350460052 CET	8.8.8.8	192.168.2.22	0x40bd	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:16.020915031 CET	8.8.8.8	192.168.2.22	0x3956	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:21.292143106 CET	8.8.8.8	192.168.2.22	0xedae	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:25.636167049 CET	8.8.8.8	192.168.2.22	0xda4c	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:30.076360941 CET	8.8.8.8	192.168.2.22	0xe283	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:30.094160080 CET	8.8.8.8	192.168.2.22	0xe283	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:30.114598036 CET	8.8.8.8	192.168.2.22	0xe283	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:34.404181957 CET	8.8.8.8	192.168.2.22	0xe3ae	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:38.734345913 CET	8.8.8.8	192.168.2.22	0xe571	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:43.026751995 CET	8.8.8.8	192.168.2.22	0x6377	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:47.482248068 CET	8.8.8.8	192.168.2.22	0x785	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:47.592971087 CET	8.8.8.8	192.168.2.22	0x785	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:47.612920046 CET	8.8.8.8	192.168.2.22	0x785	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:47.630901098 CET	8.8.8.8	192.168.2.22	0x785	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 1, 2023 22:34:52.772857904 CET	8.8.8.8	192.168.2.22	0x3c29	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:52.884701967 CET	8.8.8.8	192.168.2.22	0x3c29	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:52.902323961 CET	8.8.8.8	192.168.2.22	0x3c29	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:58.304527998 CET	8.8.8.8	192.168.2.22	0xaee9	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:58.322787046 CET	8.8.8.8	192.168.2.22	0xaee9	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:34:58.341437101 CET	8.8.8.8	192.168.2.22	0xaee9	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:02.732624054 CET	8.8.8.8	192.168.2.22	0xde9a	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:08.037184000 CET	8.8.8.8	192.168.2.22	0x6b9	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:08.057095051 CET	8.8.8.8	192.168.2.22	0x6b9	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:13.372343063 CET	8.8.8.8	192.168.2.22	0x3c9d	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:13.390119076 CET	8.8.8.8	192.168.2.22	0x3c9d	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:13.408463001 CET	8.8.8.8	192.168.2.22	0x3c9d	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:18.726483107 CET	8.8.8.8	192.168.2.22	0x617e	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:24.255112886 CET	8.8.8.8	192.168.2.22	0x7e09	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false
Feb 1, 2023 22:35:28.625910997 CET	8.8.8.8	192.168.2.22	0x3b94	No error (0)	boele.duckdns.org		45.137.65.132	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- ask6.awt.com.pk

Statistics

Behavior

- WINWORD.EXE
- EQNEDT32.EXE
- word.exe
- rnixgfly.exe
- rnixgfly.exe
- jfcarlsrvb.exe
- EQNEDT32.EXE

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: **2876**, Parent PID: **576**

General	
Target ID:	0
Start time:	22:33:19
Start date:	01/02/2023
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f4b0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Analysis Process: EQNEDT32.EXE PID: **3000**, Parent PID: **576**

General	
Target ID:	2
Start time:	22:33:20
Start date:	01/02/2023
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Roaming\word.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6062CF	URLDownloadToFileW

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\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\stanmac2.1[1].exe	0	759	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 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	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPgLPf*_;PfsVPf.V`PfRichPfPELOah*	success or wait	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\stanmac2.1[1].exe	759	4120	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 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 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 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 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 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 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 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 00 00 00 00 00 00 00 00		success or wait	1	6062CF	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\word.exe	0	4879	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 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	MZ@!L!This program cannot be run in DOS mode.$1PfPfPf*_9PfPg LPf*_;PfsVPf.V`PfRichPf PELOah*	success or wait	1	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\stanmac2.1[1].exe	6165	6430	00 50 68 fd 03 00 00 fd 45 08 57 50 fd 75 fd 56 fd 15 50 fd 40 00 66 fd 3f 0a fd 1d fd fd fd 39 5d fd fd 75 fd 75 2b 6a 02 fd 09 00 00 fd fd 3b fd 0f fd fd 04 00 00 6a 33 fd 52 09 00 00 50 56 fd 15 14 fd 40 00 56 fd fd fd 15 10 fd 40 00 fd 16 6a 22 fd 38 09 00 00 fd 4d fd fd fd 51 50 56 fd fd 09 00 00 fd fd 3b fd 0f fd fd 07 00 00 fd 04 00 00 fd 75 fd fd fd fd 45 fd 6a 02 fd 45 fd fd 0a 09 00 00 6a 11 fd 45 fd fd 00 09 00 00 6a 02 50 57 fd 45 fd 01 00 00 00 fd 09 00 00 3b c9 45 08 0f fd 69 07 00 00 33 fd fd fd 01 fd fd fd 40 00 75 11 6a 23 fd fd 08 00 00 57 fd 41 00 00 fd 44 00 02 fd fd 04 75 12 6a 03 fd 08 00 00 59 fd fd fd 40 00 56 fd 55 fd 58 fd fd 03 75 0f 68 00 18 00 00 57 53 fd 75 fd fd 68 0e 00 00 50 57 fd 75 fd 53 fd 75 fd fd 75	PhEWPuVP@f? 9]uu+j;j3RPV@V@j"8M QPV;uEjEjEjPWE;Ei3@uj #WADujY@V UXuhWSuhPWuSuu	success or wait	66	6062CF	URLDownloadToFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\word.exe	4879	10288	0d 00 00 53 fd 0e 00 00 6a 31 fd fd 0e 00 00 6a 22 fd fd 7c 0e 00 00 6a 15 fd fd fd 73 0e 00 00 6a fd fd fd fd fd fd 45 fd fd fd 78 fd fd fd 45 fd fd fd 7c fd fd fd 45 09 45 fd 66 fd 06 66 fd fd 1b fd fd 5d fd 23 89 45 fd 66 fd 07 66 fd fd 1b fd fd 45 fd 00 60 43 00 23 c9 45 fd fd fd 74 fd fd fd 50 fd 0c 3d 00 00 fd fd 0f fd fd 09 00 00 fd fd 78 fd fd fd 40 0f fd fd 0c 00 00 fd 75 fd fd 41 4b 00 00 fd 75 fd fd 47 53 fd fd 0d 00 00 fd fd 56 6a fd fd 16 37 00 00 56 fd 3c 00 00 fd fd 3b fd 0f fd 6a 09 00 00 39 5d fd 74 21 56 fd 11 4b 00 00 39 5d fd 7c 0b 50 fd 75 fd fd fd 45 00 00 fd 0b 3b fd 74 07 fd 45 fd 01 00 00 00 56 fd 15 24 fd 40 00 fd 34 0c 00 00 6a 02 fd 0d 00 00 50 fd 49 00 00 fd fd 3b fd 74 13 fd 76 14 fd 75	Sj1j"|jsjExE|EEff]#EffE`C #EtP= x@uAKuGSVj7V<;j9]t!VK 9]|PuE;tEV$@4jPI;tvu	success or wait	9	6062CF	URLDownloadToFileW
C:\Users\user\AppData\Roaming\word.exe	327680	102349	1c fd 7d fd fd 05 fd fd 4c 58 1c fd 0b 69 fd 02 7c 2c fd 00 27 04 fd fd 76 5a 07 41 29 0c fd 22 79 fd 71 fd 09 fd fd 52 18 7b 27 fd 53 0e ff 45 3f 6a fd 0e fd 3f 5e fd fd 10 fd 7e 57 fd fd fd 6d 6b fd 84 42 fd fd fd fd 0e fd fd 74 fd 44 fd fd fd 44 fd 2d fd fd fd 51 fd fd fd 27 fd 31 3e fd 49 08 7b fd fd 69 53 fd 39 fd fd fd 36 1f 24 59 08 fd fd fd 63 fd 7b fd fd 1f 78 99 78 1f 75 fd fd 53 fd 1e 74 79 fd fd 1c fd 0e 7d 6f 3f 4e 7d 0b 3b 69 fd 43 fd 6a fd 68 2d 5d fd 16 fd 6f 76 0b 20 fd 3a fd fd fd fd fd fd 5b fd 41 67 04 fd fd fd 0e fd fd 5e fd 47 1b 3c fd 23 54 68 54 fd 21 5f c7 fd e3 69 78 4b 5f 20 fd 79 fd 06 5a fd cb 3b fd 1a fd 21 5d fd 06 fd fd fd fd fd fd 02 25 fd 70 fd 64 4c fd 16 fd fd 0f fd 64 fd fd fd	}LXi|,'ZA)"yqR{'SE?j? ^~WmkBtDD-Q'1>I{i96$Yc{xxuSty}o? N};iCjh-]ov : [Ag^G<#ThT!_ixK_ yZ;!]%pdLd	success or wait	1	6062CF	URLDownloadToFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: word.exe PID: **2848**, Parent PID: **3000**

General

Target ID:	5
Start time:	22:33:25

Start date:	01/02/2023
Path:	C:\Users\user\AppData\Roaming\word.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\word.exe
Imagebase:	0x400000
File size:	430029 bytes
MD5 hash:	D3E933B0AAB571BDC73355A106D657E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 65%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsr3DEB.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsl3E1A.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsl3E1B.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	4061C6	GetTempFileNameW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsl3E1B.tmp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405BE2	CreateDirectoryW
C:\Users	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405C22	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\vvnwaf.f	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW
C:\Users\user\AppData\Local\Temp\rnixgfly.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	406184	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsr3DEB.tmp	success or wait	1	403988	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsl3E1B.tmp	success or wait	1	405DA3	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsl3E1A.tmp	0	28785	26 36 00 00 fd 00 00 00 2c 01 00 00 02 00 00 00 fd 01 00 00 03 00 00 00 fd 19 00 00 79 00 00 00 30 27 00 00 00 00 00 00 40 35 00 00 01 00 00 00 0e 36 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 fd fd fd fd fd fd fd fd fd 00 00 00 00 00 fd 00 00 fd 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 1c 00 00 00 fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd fd 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 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 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	&6,y0'@56	success or wait	21	406224	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\vvnwaf.f	0	16384	43 73 fd fd 03 77 fd 57 37 fd 33 fd 3d 51 fd 09 08 fd 81 34 fd fd fd 4c 22 fd 4f fd 10 24 4a 7b fd fd 7b fd fd 11 7a fd fd fd fd fd 23 fd 03 2b fd 45 fd fd 34 0b fd 1c 59 fd fd fd 36 fd 29 1c 50 1f 38 6a 0a fd 5e fd 1b fd fd fd 59 fd fd 4d fd 13 6d fd 76 0d 34 41 49 fd 01 2a fd 70 fd 38 fd fd 69 fd 4d 35 fd 5a 2d 75 0e fd 71 fd fd 22 a6 47 e2 3e 19 fd 77 71 18 1a 07 44 fd fd fd 76 03 21 57 fd 62 58 36 fd 2b fd fd 66 fd fd fd fd fd fd 3e 23 75 52 53 3e fd 7e 33 fd 24 4f 74 79 fd 7d fd 57 65 4c 14 5d fd 74 fd fd 6f f2 fd fd 59 fd 46 fd 53 fd 46 fd 03 47 fd fd 6b fd fd fd 67 16 fd fd fd 22 1c fd fd 53 2e 11 53 fd fd fd fd 24 fd 1b 01 fd 18 04 fd fd fd 34 68 fd fd fd fd fd 68 28 fd 22 fd fd fd 27 fd	CswW73=Q4L"O$J{(#+E 4Y6)P8^YMmv 4AI*p8iM5Z- uq"G>wqDv!WbX+f>#uR S>~3$Oty}WeL]toYFSFG kg"S.S$4hh"'	success or wait	19	406224	WriteFile
C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt	0	7840	e3 37 30 35 6d fd fd 66 fd 46 3c fd 12 1b 30 35 6f fd 3a fd fd fd fd fd fd 3f 76 3e fd 33 fd 33 fd 3c fd 0c fd fd fd fd 4d fd 6b 6e 6c fd 30 32 61 fd fd 63 fd 45 3c fd 17 10 34 32 63 fd 20 fd fd fd fd fd fd 34 fd 44 36 33 fd 36 fd 33 fd 3f fd 0d fd fd fd 45 fd 67 6e 69 fd 35 33 50 fd 04 38 30 35 fd 70 38 fd 71 3f fd 32 fd 38 fd 75 20 fd 61 fd fd 62 65 61 62 6f fd 48 30 03 bb 76 0f fd 76 0c 40 33 fd 60 14 fd 69 2f 37 fd 70 14 36 fd 74 28 32 fd fd 67 31 7d 71 75 3c fd fd 47 2d fd 30 fd 33 fd 68 fd 66 fd fd fd 0f 77 38 4c 24 fd 6d fd 72 0b 44 3b 46 fd 07 fd 6f 6b 63 fd fd 6d fd 3b 34 fd 71 fd 3f fd 3c 40 fd 34 fd 30 fd fd fd 6d fd 73 75 3c 66 fd f1 fd 40 25 fd 60 34 fd fd 44 27 64 fd 4f 24 fd fd 41 35 1b fd 3d 01 fd 3c 72 fd	705mfF<05o:? v>33<Mknl02acE<42c 4D6363? Egni53P805p8q?28u abea boH0vv@3`i/7p6t(2g}u<G -03hfw8L $mrD;Fokcm;4q? <@40mu<f@%`4D'dO $A5=<r	success or wait	1	406224	WriteFile
C:\Users\user\AppData\Local\Temp\rnixgfly.exe	0	16384	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 4f 65 38 25 0b 04 56 76 0b 04 56 76 0b 04 56 76 64 72 fd 76 2b 04 56 76 64 72 fd 76 18 04 56 76 02 7c fd 76 1e 04 56 76 0b 04 57 76 fd 04 56 76 64 72 fd 76 7c 04 56 76 64 72 fd 76 0a 04 56 76 52 69 63 68 0b 04 56 76 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 63 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$Oe8%VvVvVvdrv + VvdrvVv|vVvWvVvdrv|Vv drvVvRichVvPELc	success or wait	5	406224	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\word.exe	unknown	512	success or wait	208	4061F5	ReadFile
C:\Users\user\AppData\Roaming\word.exe	unknown	16384	success or wait	20	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsl3E1A.tmp	unknown	4	success or wait	1	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsl3E1A.tmp	unknown	13862	success or wait	1	40345F	ReadFile
C:\Users\user\AppData\Local\Temp\nsl3E1A.tmp	unknown	4	success or wait	3	4061F5	ReadFile
C:\Users\user\AppData\Local\Temp\nsl3E1A.tmp	unknown	16384	success or wait	25	4061F5	ReadFile

Analysis Process: rnixgfly.exe PID: **2036**, Parent PID: **2848**

General

Target ID:	6
Start time:	22:33:25
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\rnixgfly.exe" C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	C1DC97853E14C21B463C6E95B21C300C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000006.00000002.927611273.0000000000380000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000006.00000002.927611273.0000000000380000.00000004.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000006.00000002.927611273.0000000000380000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000006.00000002.927611273.0000000000380000.00000004.00001000.00020000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.927611273.0000000000380000.00000004.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.927611273.0000000000380000.00000004.00001000.00020000.00000000.sdmp, Author: unknown
Antivirus matches:	• Detection: 41%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ilkqegcy	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	220414	CreateDirectoryW
C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	220357	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\Roaming\ilkqegcy\jfcarlsrvb.exe	0	76800	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 4f 65 38 25 0b 04 56 76 0b 04 56 76 0b 04 56 76 64 72 fd 76 2b 04 56 76 64 72 fd 76 18 04 56 76 02 7c fd 76 1e 04 56 76 0b 04 57 76 fd 04 56 76 64 72 fd 76 7c 04 56 76 64 72 fd 76 0a 04 56 76 52 69 63 68 0b 04 56 76 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 03 00 fd fd fd 63 00 00 00 00 00 00 00 00 00 fd 00 03 01 0b 01 0a 00 00 fd 00	MZ@!L!This program cannot be run in DOS mode.$Oe8%VvVvVvdrv + VvdrvVv|vVvWvVvdrv|VvdrvVvRichVvPELc	success or wait	1	220366	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt	unknown	4096	success or wait	1	40528A	ReadFile
C:\Users\user\AppData\Local\Temp\somvwkehjlp.rt	unknown	4096	success or wait	1	40528A	ReadFile
C:\Users\user\AppData\Local\Temp\rnixgfly.exe	unknown	76800	success or wait	1	220339	ReadFile
C:\Users\user\AppData\Local\Temp\vvnwaf.f	unknown	287232	success or wait	1	22124E	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2216C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2216C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2216C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2216C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2216C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2216C1	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	2216C1	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	ryhcwrfexidnfv	unicode	C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe "C:\Users\user\AppData\Local\Temp\rnixgfly.exe" C:\Users\user\AppData\Loc	success or wait	1	2208D5	RegSetValueExW

Analysis Process: rnixgfly.exe PID: **2116**, Parent PID: **2036**

General

Target ID:	7
Start time:	22:33:26
Start date:	01/02/2023
Path:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\rnixgfly.exe
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	C1DC97853E14C21B463C6E95B21C300C
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: 00000007.00000002.1188366670.00000000065A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1188366670.00000000065A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1188366670.00000000065A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1188366670.00000000065A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1188464789.00000000065D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1188464789.00000000065D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1188464789.00000000065D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1188464789.00000000065D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1187506005.00000000056F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1187506005.00000000056F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1187506005.00000000056F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1187506005.00000000056F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1187014701.00000000046B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1187014701.00000000046B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1187014701.00000000046B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1187014701.00000000046B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1187252791.0000000004DF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1187252791.0000000004DF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1187252791.0000000004DF0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1187252791.0000000004DF0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1187866924.00000000059D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1187866924.00000000059D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1187866924.00000000059D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1187866924.00000000059D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1188403629.00000000065B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1188403629.00000000065B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1188403629.00000000065B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1188403629.00000000065B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1188248716.0000000006570000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1188248716.0000000006570000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1188248716.0000000006570000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1188248716.0000000006570000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1186150813.000000000328B000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1186150813.000000000328B000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1186150813.000000000328B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1182625112.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1182625112.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1182625112.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1182625112.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1182625112.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1182625112.0000000000400000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1188336607.0000000006590000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1188336607.0000000006590000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1188336607.0000000006590000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1188336607.0000000006590000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1186150813.0000000003523000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1186150813.0000000003523000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1188430704.00000000065C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1188430704.00000000065C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1188430704.00000000065C0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1188430704.00000000065C0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1188274137.0000000006580000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1188274137.0000000006580000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1188274137.0000000006580000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1188274137.0000000006580000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1187329723.0000000005000000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1187329723.0000000005000000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1187329723.0000000005000000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1187329723.0000000005000000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1187329723.0000000005000000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1188521555.0000000006610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1188521555.0000000006610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1188521555.0000000006610000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1188521555.0000000006610000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000007.00000003.1075179534.0000000003677000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000003.1075179534.0000000003677000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1183458585.000000000227B000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1183458585.000000000227B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1183458585.0000000002211000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1183458585.0000000002211000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1183225177.0000000001EB2000.00000040.00001000.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1183225177.0000000001EB2000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1183225177.0000000001EB2000.00000040.00001000.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1183225177.0000000001EB2000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1187463835.00000000056D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1187463835.00000000056D0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1187463835.00000000056D0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1187463835.00000000056D0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1186150813.0000000003211000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1182833387.0000000000603000.00000004.00000020.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1182833387.0000000000603000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1182833387.0000000000603000.00000004.00000020.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1182833387.0000000000603000.00000004.00000020.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.1183154390.0000000001E70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000007.00000002.1183154390.0000000001E70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.1183154390.0000000001E70000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000007.00000002.1183154390.0000000001E70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: NanoCore, Description: unknown, Source: 00000007.00000002.1183154390.0000000001E70000.00000004.08000000.00040000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000007.00000002.1183154390.0000000001E70000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	70B64247	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	70B6F4A8	CreateFileW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	70B64247	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\Logs\user	read data or list directory | synchronize	device | sparse file	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	70B64247	CreateDirectoryW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\catalog.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	23	70B6F4A8	CreateFileW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	70B6F4A8	CreateFileW
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\settings.bin	read attributes | synchronize | generic write	device | sparse file	synchronous io non alert | non directory file | open no recall	success or wait	1	70B6F4A8	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\run.dat	0	8	fd fd 7e 66 fd 04 fd 48	~fH	success or wait	1	70B6B2B3	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\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	23	70B6B2B3	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^Qoy=e@9BF09u"30tRDn_4dEi~|fX_Xfp^>a$e6:7d(aA=)*{B[y%*iQ<xtXHHF7gI*3{nLy;is-(5iJ5b7}fKHV	success or wait	1	70B6B2B3	WriteFile
C:\Users\user\AppData\Roaming\EA860E7A-A87F-4A88-92EF-38F744458171\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	70B6B2B3	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	72E27995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72E27995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D3DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72E2A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	72D3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	72D3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	72D3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	72D3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D3DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D3DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	70B6B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	70B6B2B3	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	72D512BF	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System\v4.0_4.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	72D512BF	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	72D3DE2C	ReadFile

Analysis Process: jfcarlsrvb.exe PID: **2216**, Parent PID: **1860**

General

Target ID:	8
Start time:	22:33:38

Start date:	01/02/2023
Path:	C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\ilkqegcy\jfcarlsrvb.exe" "C:\Users\user\AppData\Local\Temp\rnixgfly.exe" C:\Users\user\AppData\Lo
Imagebase:	0x400000
File size:	76800 bytes
MD5 hash:	C1DC97853E14C21B463C6E95B21C300C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	• Detection: 41%, ReversingLabs
Reputation:	low

Analysis Process: EQNEDT32.EXE PID: **1972**, Parent PID: **576**

General

Target ID:	11
Start time:	22:33:51
Start date:	01/02/2023
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly