ID: 714139
Sample Name:
G62PnhPS1s.exe
Cookbook: default.jbs
Time: 17:06:16
Date: 01/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

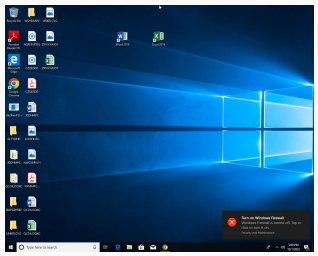
Windows Analysis Report

G62PnhPS1s.exe

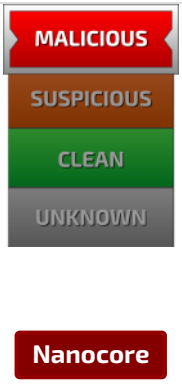
Overview

General Information

Sample Name:	G62PnhPS1s.exe
Analysis ID:	714139
MD5:	07653fd9f64401f..
SHA1:	aed898c8d28306..
SHA256:	34915a0eded4e5.
Tags:	exe NanoCore RAT
Infos:	



Detection



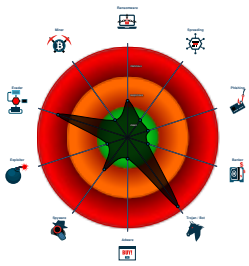
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Sigma detected: Scheduled temp fil…
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Hides threads from debuggers
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- G62PnhPS1s.exe (PID: 5512 cmdline: C:\Users\user\Desktop\G62PnhPS1s.exe MD5: 07653FD9F64401F9F1696F4782C926F4)
  - schtasks.exe (PID: 5552 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpF33C.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5560 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5604 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpF531.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5612 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- G62PnhPS1s.exe (PID: 5688 cmdline: C:\Users\user\Desktop\G62PnhPS1s.exe 0 MD5: 07653FD9F64401F9F1696F4782C926F4)
- dhcpmon.exe (PID: 5708 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 07653FD9F64401F9F1696F4782C926F4)
- dhcpmon.exe (PID: 5816 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 07653FD9F64401F9F1696F4782C926F4)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
G62PnhPS1s.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x12e8ed:$s1: \x02\x1E\x1E\x1APEE

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	SUSP_XORed_URL_in_EXE	Detects an XORed URL in an executable	Florian Roth	• 0x12e8ed:$s1: \x02\x1E\x1E\x1APEE

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xf778:$x2: NanoCore.ClientPlugin • 0xf7ad:$x3: NanoCore.ClientPluginHost • 0xf76c:$i2: IClientData • 0xf78e:$i3: IClientNetwork • 0xf79d:$i5: IClientDataHost • 0xf7c7:$i6: IClientLoggingHost • 0xf7da:$i7: IClientNetworkHost • 0xf7ed:$i8: IClientUIHost • 0xf7fb:$i9: IClientNameObjectCollection • 0xf817:$i10: IClientReadOnlyNameObjectCollection • 0xf56a:$s1: ClientPlugin • 0xf781:$s1: ClientPlugin • 0x147a2:$s6: get_ClientSettings
00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xf7ad:$a1: NanoCore.ClientPluginHost • 0xf778:$a2: NanoCore.ClientPlugin • 0x146f3:$b1: get_BuilderSettings • 0x14662:$b7: LogClientException • 0xf7c7:$b9: IClientLoggingHost
Click to see the 24 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.G62PnhPS1s.exe.5d64629.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
0.2.G62PnhPS1s.exe.5d64629.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost
0.2.G62PnhPS1s.exe.5d64629.5.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.G62PnhPS1s.exe.5d64629.5.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0xb14f:$x2: NanoCore.ClientPlugin • 0xb184:$x3: NanoCore.ClientPluginHost • 0xb143:$i2: IClientData • 0xb165:$i3: IClientNetwork • 0xb174:$i5: IClientDataHost • 0xb19e:$i6: IClientLoggingHost • 0xb1b1:$i7: IClientNetworkHost • 0xb1c4:$i8: IClientUIHost • 0xb1d2:$i9: IClientNameObjectCollection • 0xb1ee:$i10: IClientReadOnlyNameObjectCollection • 0xaf41:$s1: ClientPlugin • 0xb158:$s1: ClientPlugin • 0x10179:$s6: get_ClientSettings
0.2.G62PnhPS1s.exe.5d64629.5.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0xb184:$a1: NanoCore.ClientPluginHost • 0xb14f:$a2: NanoCore.ClientPlugin • 0x100ca:$b1: get_BuilderSettings • 0x10039:$b7: LogClientException • 0xb19e:$b9: IClientLoggingHost
Click to see the 40 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Persistence and Installation Behavior

Sigma detected: Scheduled temp file as task from temp location

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049701277252025019 10/01/22-17:08:43.514254
SID:	2025019
Source Port:	49701
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049682277252816766 10/01/22-17:07:16.118415
SID:	2816766
Source Port:	49682
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049700277252025019 10/01/22-17:08:36.499125
SID:	2025019
Source Port:	49700
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049702277252025019 10/01/22-17:08:49.653446
SID:	2025019
Source Port:	49702
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049691277252816766 10/01/22-17:07:48.171991
SID:	2816766
Source Port:	49691
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049693277252816766 10/01/22-17:08:00.702896
SID:	2816766
Source Port:	49693
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049683277252816766 10/01/22-17:07:22.198867
SID:	2816766
Source Port:	49683
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049690277252816766 10/01/22-17:07:41.862031
SID:	2816766
Source Port:	49690
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049694277252816766 10/01/22-17:08:06.673277
SID:	2816766
Source Port:	49694
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049706277252025019 10/01/22-17:09:18.912433
SID:	2025019
Source Port:	49706
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049692277252816766 10/01/22-17:07:54.614534
SID:	2816766
Source Port:	49692
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049705277252025019 10/01/22-17:09:12.475195
SID:	2025019
Source Port:	49705
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049690277252025019 10/01/22-17:07:40.062280
SID:	2025019
Source Port:	49690

Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	−
Timestamp:	192.168.2.4209.25.141.18049704277252025019 10/01/22-17:09:03.717769
SID:	2025019
Source Port:	49704
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	−
Timestamp:	192.168.2.4209.25.141.18049703277252025019 10/01/22-17:08:56.029202
SID:	2025019
Source Port:	49703
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	−
Timestamp:	192.168.2.4209.25.141.18049691277252025019 10/01/22-17:07:46.508056
SID:	2025019
Source Port:	49691
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	−
Timestamp:	192.168.2.4209.25.141.18049692277252025019 10/01/22-17:07:52.816553
SID:	2025019
Source Port:	49692
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	−
Timestamp:	192.168.2.4209.25.141.18049700277252816766 10/01/22-17:08:38.523559
SID:	2816766
Source Port:	49700
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	−
Timestamp:	192.168.2.4209.25.141.18049683277252025019 10/01/22-17:07:20.412264
SID:	2025019
Source Port:	49683
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	−
Timestamp:	192.168.2.4209.25.141.18049693277252025019 10/01/22-17:07:58.856083
SID:	2025019
Source Port:	49693
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049694277252025019 10/01/22-17:08:04.907694
SID:	2025019
Source Port:	49694
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049682277252025019 10/01/22-17:07:14.309819
SID:	2025019
Source Port:	49682
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049684277252025019 10/01/22-17:07:26.854755
SID:	2025019
Source Port:	49684
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049697277252816718 10/01/22-17:08:25.131746
SID:	2816718
Source Port:	49697
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049701277252816766 10/01/22-17:08:45.444375
SID:	2816766
Source Port:	49701
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049682277252816718 10/01/22-17:07:16.118415
SID:	2816718
Source Port:	49682
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049702277252816766 10/01/22-17:08:51.692619
SID:	2816766
Source Port:	49702
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049703277252816766 10/01/22-17:08:59.559197
SID:	2816766
Source Port:	49703

Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	▬
Timestamp:	192.168.2.4209.25.141.18049697277252025019 10/01/22-17:08:23.697702
SID:	2025019
Source Port:	49697
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	▬
Timestamp:	192.168.2.4209.25.141.18049695277252025019 10/01/22-17:08:11.265098
SID:	2025019
Source Port:	49695
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	▬
Timestamp:	192.168.2.4209.25.141.18049696277252025019 10/01/22-17:08:17.220015
SID:	2025019
Source Port:	49696
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	▬
Timestamp:	192.168.2.4209.25.141.18049704277252816766 10/01/22-17:09:05.788694
SID:	2816766
Source Port:	49704
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	▬
Timestamp:	192.168.2.4209.25.141.18049689277252816766 10/01/22-17:07:35.720837
SID:	2816766
Source Port:	49689
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	▬
Timestamp:	192.168.2.4209.25.141.18049705277252816766 10/01/22-17:09:14.827870
SID:	2816766
Source Port:	49705
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	▬
Timestamp:	192.168.2.4209.25.141.18049698277252816766 10/01/22-17:08:31.982437
SID:	2816766
Source Port:	49698
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049698277252025019 10/01/22-17:08:29.909653
SID:	2025019
Source Port:	49698
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049684277252816766 10/01/22-17:07:29.595955
SID:	2816766
Source Port:	49684
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049695277252816766 10/01/22-17:08:12.935261
SID:	2816766
Source Port:	49695
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049697277252816766 10/01/22-17:08:25.559661
SID:	2816766
Source Port:	49697
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049689277252025019 10/01/22-17:07:33.797666
SID:	2025019
Source Port:	49689
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 209.25.141.180	
Timestamp:	192.168.2.4209.25.141.18049696277252816766 10/01/22-17:08:19.169513
SID:	2816766
Source Port:	49696
Destination Port:	27725
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

PE file has nameless sections

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Anti Debugging

Hides threads from debuggers

Tries to detect sandboxes and other dynamic analysis tools (window names)

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

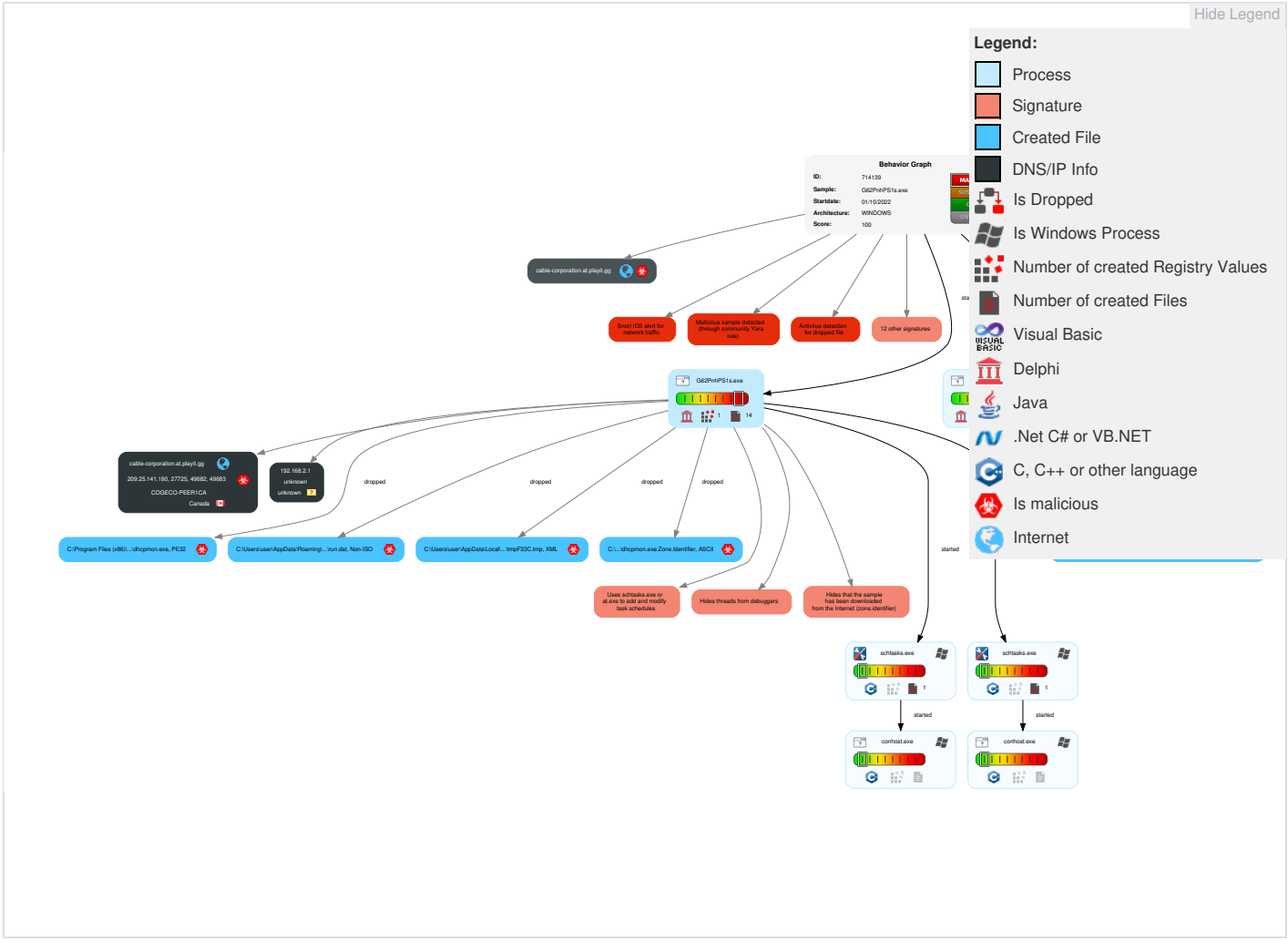
Yara detected Nanocore RAT

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 Scheduled Task/Job	1 Scheduled Task/Job	1 Access Token Manipulation	2 Masquerading	2 1 Input Capture	3 1 1 Security Software Discovery	Remote Services	2 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

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	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 2 Process Injection	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Scheduled Task/Job	2 3 1 Virtualization/Sandbox Evasion	Security Account Manager	2 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Access Token Manipulation	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 2 Process Injection	LSA Secrets	3 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	1 Non-Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	1 Application Layer Protocol	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Hidden Files and Directories	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 Obfuscated Files or Information	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 3 Software Packing	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

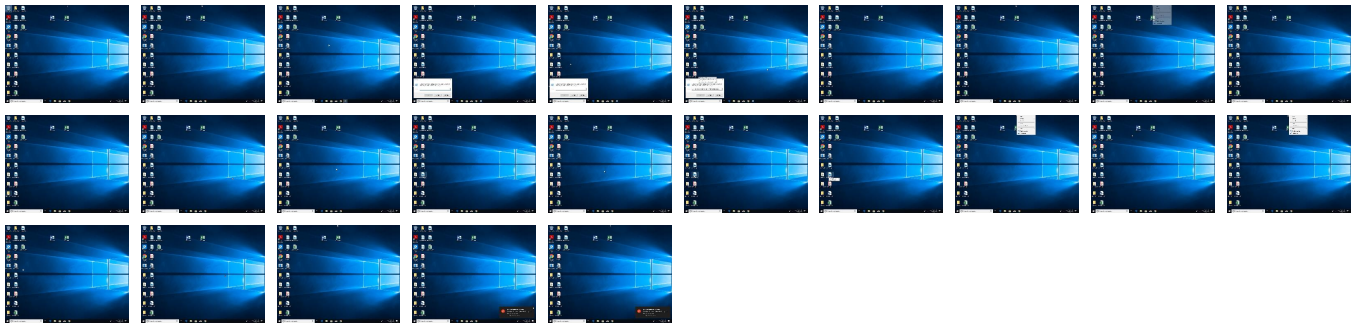
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
G62PnhPS1s.exe	85%	ReversingLabs	Win32.Backdoor.NanoCore	
G62PnhPS1s.exe	51%	Virustotal		Browse
G62PnhPS1s.exe	100%	Avira	HEUR/AGEN.1215957	
G62PnhPS1s.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	HEUR/AGEN.1215957	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	85%	ReversingLabs	Win32.Backdoor.NanoCore	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	51%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.G62PnhPS1s.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1215901		Download File

Source	Detection	Scanner	Label	Link	Download
0.2.G62PnhPS1s.exe.5d60000.4.unpack	100%	Avira	TR/NanoCore.fadte		Download File
5.2.G62PnhPS1s.exe.432000.1.unpack	100%	Avira	TR/Patched.Ren.Gen2		Download File
5.2.G62PnhPS1s.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1208316		Download File

Domains

Source	Detection	Scanner	Label	Link
cable-corporation.at.playit.gg	5%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.enigmaprotector.com/	0%	URL Reputation	safe	
http://www.enigmaprotector.com/openU	0%	URL Reputation	safe	

Domains and IPs

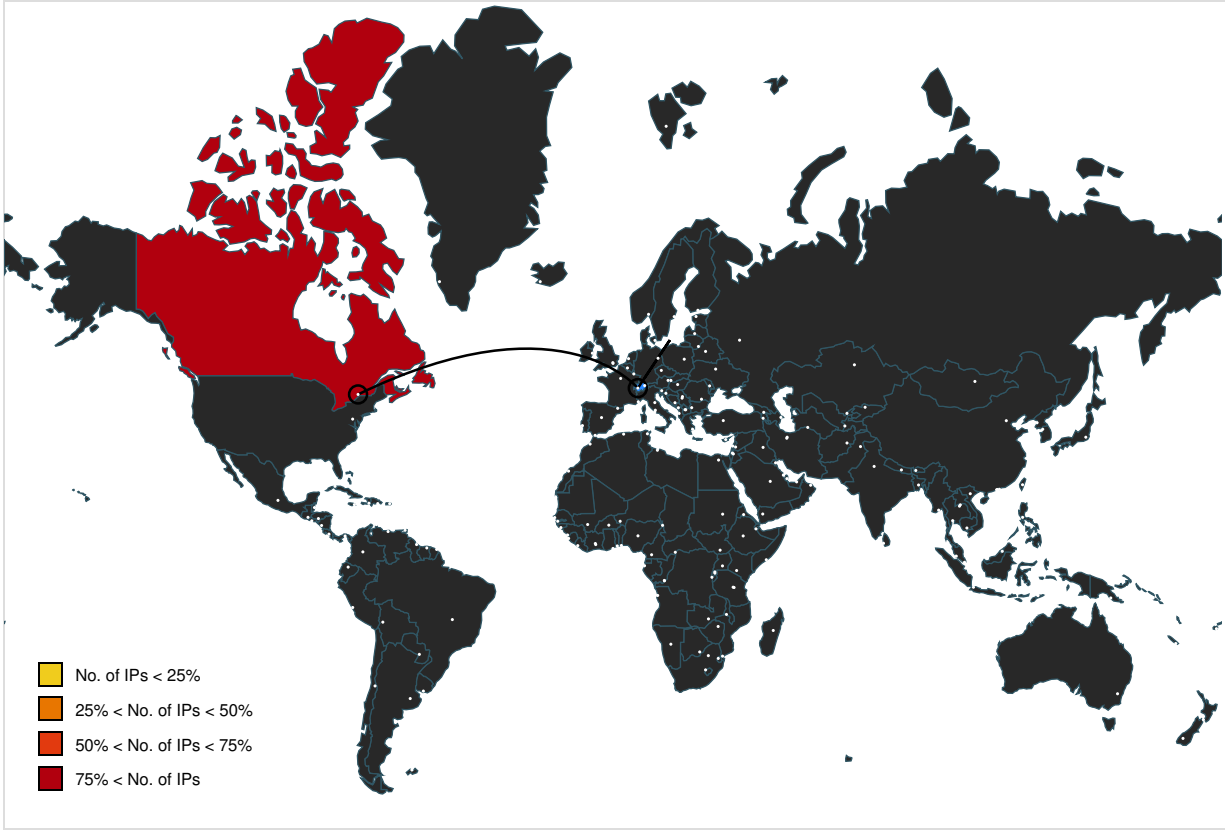
Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cable-corporation.at.playit.gg	209.25.141.180	true	true	• 5%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.enigmaprotector.com/	G62PnhPS1s.exe, 00000005.00000002.324685861.0000000000432000.00000040.00000001.01000000.00000003.sdmp, dhcpmon.exe, 00000006.00000002.327616554.0000000000791000.00000040.00000001.01000000.00000005.sdmp	false	• URL Reputation: safe	unknown
http://www.enigmaprotector.com/openU	G62PnhPS1s.exe, 00000005.00000002.324685861.0000000000432000.00000040.00000001.01000000.00000003.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.25.141.180	cable-corporation.at.playit.gg	Canada		13768	COGECO-PEER1CA	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	714139
Start date and time:	2022-10-01 17:06:16 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	G62PnhPS1s.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL

Classification:	mal100.troj.evad.winEXE@10/8@20/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 53.2% (good quality ratio 52.7%) • Quality average: 79.4% • Quality standard deviation: 25.8%
HCA Information:	• Successful, ratio: 65% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
17:07:13	API Interceptor	897x Sleep call for process: G62PnhPS1s.exe modified
17:07:14	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\G62PnhPS1s.exe" s>$(Arg0)
17:07:14	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
17:07:16	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\G62PnhPS1s.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	1246208
Entropy (8bit):	**7.990780186599993**
Encrypted:	**true**
SSDEEP:	24576:wUeIzt/bfQ8OBromXFprxo3FFkBuK/qI/nJi6CYyHFBgsnfLum9My3o54TRM+:4xUC8FU3XkBuAdfsYybggfL/Gx
MD5:	07653FD9F64401F9F1696F4782C926F4
SHA1:	AED898C8D28306AA28785004252B81144BB73676
SHA-256:	34915A0EDED4E59CFD552AE7724E99584EC58F24B8A562FD90AA6DCB9397A019
SHA-512:	96178C05A5F78F3C132E9634957194C4D90BDE07413FFD086DE05AD3B638188132C40F84112949AB31818FFBB578980F99A938990846EC70061D5513732894F0
Malicious:	**true**
Yara Hits:	• Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 85% • Antivirus: Virustotal, Detection: 51%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....H...b.....<.... .....@.. .....@ 9..... .+.....X.....+.....`... .....@.....`.....`.....@..... ....@....rsrc.... .....@.....'.. .....@....random..@....+..2.....@.....$...o(..6./}..... ....

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

Process:	C:\Users\user\Desktop\G62PnhPS1s.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\G62PnhPS1s.exe.log

Process:	C:\Users\user\Desktop\G62PnhPS1s.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

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

Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmpF33C.tmp

Process:	C:\Users\user\Desktop\G62PnhPS1s.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1300
Entropy (8bit):	5.107533892792601
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0Yayxtn:cbk4oL600QydbQxIYODOLedq3Bj
MD5:	B0B51A62FC7A6CAAF2D3035423C0CD81
SHA1:	818AC6EB9B12FE5C4832855B88F1CFEA973EC944
SHA-256:	FE02E823C955C7E5A8917B34695129A5EEB33B2254ECEA586B8D425AF0AF569F
SHA-512:	53465207ED52E68CC3BBC095EE9FB075E97B2DE7A50935705C84E1B1CF4523F01F93983278D5B59CB2C81C2935F67E545698A073D9D4CAA6C02237DCC6C5D46
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpF531.tmp

Process:	C:\Users\user\Desktop\G62PnhPS1s.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755734
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

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

Process:	C:\Users\user\Desktop\G62PnhPS1s.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators

Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Zqbwn:4cn
MD5:	A0B8F4FC2F080D11563C79396A5EF9FE
SHA1:	1D0AB1B41755B425DC2E4F16EA88D3F493762728
SHA-256:	993554FFED3627C4467DDE6B9F8088D2A3226D16296336A7A60C98037EB18CFA
SHA-512:	742E47CDCC74751550786DB6F9A949F5CD99C1AE5F0843CEF319A8734079EA82BC0DA631458FFAAF9BA5479BC4E59C254DC25BF552FBFFBF606CB48CAFFDCAEE
Malicious:	**true**
Preview:	.Y....H

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

Process:	C:\Users\user\Desktop\G62PnhPS1s.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	37
Entropy (8bit):	4.203526853497231
Encrypted:	false
SSDEEP:	3:oNt+WfWib1r6Jn:oNwvib1E
MD5:	351D2E4CAAA1B21ED424549F35280788
SHA1:	9CD0BAC3AA328B8D4BA1F490F47A17BF830D01DC
SHA-256:	25767F6D2FE5F40CA47BA2402045F95303DC0C7B2263F3D0A3D16F1CDEF3568D
SHA-512:	DFEB62070C9300513EFCBDCB36F01C426FD1E8000865B53F101DA0F9927E1A476E85DA6605714AE8A7C0A849A2750F384DA3AF5E46E531351F7AD3D995450BD
Malicious:	false
Preview:	C:\Users\user\Desktop\G62PnhPS1s.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.990780186599993
TrID:	• Win32 Executable (generic) a (10002005/4) 99.94% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • VXD Driver (31/22) 0.00%
File name:	G62PnhPS1s.exe
File size:	1246208
MD5:	07653fd9f64401f9f1696f4782c926f4
SHA1:	aed898c8d28306aa28785004252b81144bb73676
SHA256:	34915a0eded4e59cfd552ae7724e99584ec58f24b8a562fd90aa6dcb9397a019
SHA512:	96178c05a5f78f3c132e9634957194c4d90bde07413ffd086de05ad3b638188132c40f84112949ab31818ffbb578980f99a938990846ec70061d5513732894f0
SSDEEP:	24576:wUelzt/bfQ8OBromXFprxo3FFkBuK/qI/nJi6CYyHFBgsnfLum9My3o54TRM+:4xUC8FU3XkBuAdfsYybggfL/Gx
TLSH:	D44533D46D10EEE5E190743043DEDE596A5DA0B40E4A481ED9BDB02BE3FE12CC345BB8
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....H...b.....<.... .....@.. .....@9.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x40b23c

Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	2e5467cba76f44a088d39f78c5e807b6

Entrypoint Preview

Instruction
call 00007F7668FF7026h
jmp 00007F7668FF6E3Eh
push 0044BB60h
push dword ptr fs:[00000000h]
mov eax, dword ptr [esp+10h]
mov dword ptr [esp+10h], ebp
lea ebp, dword ptr [esp+10h]
sub esp, eax
push ebx
push esi
push edi
mov eax, dword ptr [00466ECCh]
xor dword ptr [ebp-04h], eax
xor eax, ebp
push eax
mov dword ptr [ebp-18h], esp
push dword ptr [ebp-08h]
mov eax, dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFEh
mov dword ptr [ebp-08h], eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
ret
mov ecx, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], ecx
pop ecx
pop edi
pop edi
pop esi
pop ebx
mov esp, ebp
pop ebp
push ecx
ret
int3
int3
int3
add esp, 04h
jmp 00007F766937CEC3h
or eax, F972054Dh
lahf

Instruction
sti
imul edi, dword ptr [ecx-31h], DA10A1DAh
nop
cld
cdq
dec ebp
add byte ptr [ebp-1DBF528Eh], dl
jmp dword ptr [edi+3Bh]
and byte ptr [ecx-52h], cl
and al, 9Bh
mov seg?, word ptr [ecx+45h]
scasd
test al, 9Bh
jecxz 00007F7668FF6FD0h
sub eax, ebx
mov dword ptr [00D449A0h], eax
sub edx, dword ptr [esi+05B3BE87h]
jc 00007F7668FF6F73h
jnp 00007F7668FF6FB2h
mov ebx, A172BFEFh
dec esp
int3
lodsd
iretd
jecxz 00007F7668FF6F71h
add al, D6h
cmp al, 73h
retf
scasb
stc
mov ecx, dword ptr [edx]
add al, 36h
pop edi
add byte ptr [esi-72h], al
sub dword ptr [esi-58364CA0h], ebp

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2b0020	0x210	.random
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x30000	0x58	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2b0000	0xc	.random
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
	0x2000	0x16000	0xb000	False	0.9996004971590909	data	7.996241313774297	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x18000	0x16000	0x16000	False	1.0003995028409092	data	7.9977165676251	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x2e000	0x2000	0x200	False	1.021484375	data	7.310216660215987	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x30000	0x2000	0x200	False	0.09765625	data	0.3718787954394439	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
	0x32000	0x27e000	0x2ba00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.random	0x2b0000	0xe4000	0xe3200	False	0.996978407058338	data	7.984769720522192	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x18058	0x15f68	data		

Imports

DLL	Import
kernel32.dll	GetModuleHandleA, GetProcAddress, ExitProcess, LoadLibraryA
user32.dll	MessageBoxA
advapi32.dll	RegCloseKey
oleaut32.dll	SysFreeString
gdi32.dll	CreateFontA
shell32.dll	ShellExecuteA
version.dll	GetFileVersionInfoA
mscoree.dll	_CorExeMain

Network Behavior

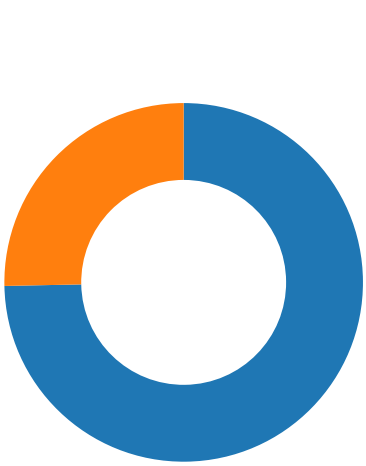
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4209.25.141.1804970127725202501910/01/22-17:08:43.514254	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.1804968227725281676610/01/22-17:07:16.118415	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49682	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.1804970027725202501910/01/22-17:08:36.499125	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.1804970227725202501910/01/22-17:08:49.653446	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	27725	192.168.2.4	209.25.141.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4209.25.141.180 49691277252816766 10/01/22-17:07:48.171991	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49691	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49693277252816766 10/01/22-17:08:00.702896	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49693	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49683277252816766 10/01/22-17:07:22.198867	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49683	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49690277252816766 10/01/22-17:07:41.862031	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49690	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49694277252816766 10/01/22-17:08:06.673277	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49694	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49706277252025019 10/01/22-17:09:18.912433	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49692277252816766 10/01/22-17:07:54.614534	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49692	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49705277252025019 10/01/22-17:09:12.475195	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49690277252025019 10/01/22-17:07:40.062280	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49690	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49704277252025019 10/01/22-17:09:03.717769	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49703277252025019 10/01/22-17:08:56.029202	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49691277252025019 10/01/22-17:07:46.508056	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49691	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49692277252025019 10/01/22-17:07:52.816553	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49692	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49700277252816766 10/01/22-17:08:38.523559	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49700	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49683277252025019 10/01/22-17:07:20.412264	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49683	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49693277252025019 10/01/22-17:07:58.856083	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49693	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49694277252025019 10/01/22-17:08:04.907694	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49694	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49682277252025019 10/01/22-17:07:14.309819	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49682	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180 49684277252025019 10/01/22-17:07:26.854755	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49684	27725	192.168.2.4	209.25.141.180

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4209.25.141.180496972772528167181 0/01/22-17:08:25.131746	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49697	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180497012772528167661 0/01/22-17:08:45.444375	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49701	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496822772528167181 0/01/22-17:07:16.118415	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49682	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180497022772528167661 0/01/22-17:08:51.692619	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180497032772528167661 0/01/22-17:08:59.559197	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496972772025019 0/01/22-17:08:23.697702	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49697	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496952772025019 0/01/22-17:08:11.265098	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49695	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496962772025019 0/01/22-17:08:17.220015	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49696	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180497042772528167661 0/01/22-17:09:05.788694	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496892772528167661 0/01/22-17:07:35.720837	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49689	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180497052772528167661 0/01/22-17:09:14.827870	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496982772528167661 0/01/22-17:08:31.982437	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49698	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496982772025019 0/01/22-17:08:29.909653	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496842772528167661 0/01/22-17:07:29.595955	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49684	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496952772528167661 0/01/22-17:08:12.935261	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49695	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496972772528167661 0/01/22-17:08:25.559661	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49697	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496892772025019 0/01/22-17:07:33.797666	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49689	27725	192.168.2.4	209.25.141.180
192.168.2.4209.25.141.180496962772528167661 0/01/22-17:08:19.169513	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49696	27725	192.168.2.4	209.25.141.180

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2022 17:07:14.197493076 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:14.217550993 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:14.218364000 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:14.309818983 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:14.543385983 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:14.853576899 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:14.873800993 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:14.878578901 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:14.977317095 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:15.015393972 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:15.153048038 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:15.153136969 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:15.290601015 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:15.290811062 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:15.428347111 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:15.428497076 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:15.568593025 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:15.568754911 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:15.706176996 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:15.706270933 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:15.843080997 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:15.843178034 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:15.980525970 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:15.980670929 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:16.118257999 CEST	27725	49682	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:16.118415117 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:16.151878119 CEST	49682	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:20.390109062 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:20.411134005 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:20.411254883 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:20.412264109 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:20.635322094 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:20.947900057 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:21.199137926 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:21.199316978 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:21.287693024 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:21.557292938 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:21.645483971 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:21.657002926 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:21.787977934 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:21.788037062 CEST	49683	27725	192.168.2.4	209.25.141.180

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2022 17:07:21.917632103 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:21.917865038 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:22.046458006 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:22.046555996 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:22.175045013 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:22.198867083 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:22.327305079 CEST	27725	49683	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:22.407402039 CEST	49683	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:26.801925898 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:26.823497057 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:26.823678017 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:26.854754925 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:27.245249987 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:27.558032036 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:27.683355093 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:28.247941017 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:28.380733967 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:28.380919933 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:28.513612986 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:28.513681889 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:28.647469997 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:28.652981997 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:28.789064884 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:28.789145947 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:28.922751904 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:28.922842979 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:29.056262016 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:29.056349039 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:29.190498114 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:29.190584898 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:29.328551054 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:29.328627110 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:29.461513996 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:29.461592913 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:29.594440937 CEST	27725	49684	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:29.595954895 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:29.610259056 CEST	49684	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:33.776952982 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:33.796523094 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:33.796725988 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:33.797666073 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:34.027232885 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:34.339660883 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:34.594789982 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:34.594961882 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:34.688628912 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:34.949069977 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:35.045114040 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:35.045214891 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:35.180012941 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:35.180094957 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:35.315352917 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:35.315531015 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:35.451826096 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:35.451922894 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:35.585154057 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:35.587045908 CEST	49689	27725	192.168.2.4	209.25.141.180
Oct 1, 2022 17:07:35.720773935 CEST	27725	49689	209.25.141.180	192.168.2.4
Oct 1, 2022 17:07:35.720837116 CEST	49689	27725	192.168.2.4	209.25.141.180

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Oct 1, 2022 17:07:14.158483982 CEST	52455	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:07:14.183562040 CEST	53	52455	8.8.8.8	192.168.2.4
Oct 1, 2022 17:07:20.279519081 CEST	63467	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:07:20.387448072 CEST	53	63467	8.8.8.8	192.168.2.4
Oct 1, 2022 17:07:26.781613111 CEST	50445	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:07:26.800611973 CEST	53	50445	8.8.8.8	192.168.2.4
Oct 1, 2022 17:07:33.757738113 CEST	50982	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:07:33.775125980 CEST	53	50982	8.8.8.8	192.168.2.4
Oct 1, 2022 17:07:40.021703005 CEST	60080	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:07:40.041121006 CEST	53	60080	8.8.8.8	192.168.2.4
Oct 1, 2022 17:07:46.452584028 CEST	61105	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:07:46.469997883 CEST	53	61105	8.8.8.8	192.168.2.4
Oct 1, 2022 17:07:52.770283937 CEST	56572	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:07:52.793500900 CEST	53	56572	8.8.8.8	192.168.2.4
Oct 1, 2022 17:07:58.805419922 CEST	50911	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:07:58.824583054 CEST	53	50911	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:04.847346067 CEST	59683	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:04.881993055 CEST	53	59683	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:11.204330921 CEST	64167	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:11.232418060 CEST	53	64167	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:17.174144030 CEST	58565	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:17.193731070 CEST	53	58565	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:23.640496969 CEST	52239	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:23.669296980 CEST	53	52239	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:29.868820906 CEST	61007	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:29.888377905 CEST	53	61007	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:36.457030058 CEST	60686	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:36.474857092 CEST	53	60686	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:43.453597069 CEST	61124	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:43.482404947 CEST	53	61124	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:49.599940062 CEST	59444	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:49.623954058 CEST	53	59444	8.8.8.8	192.168.2.4
Oct 1, 2022 17:08:55.983712912 CEST	55570	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:08:56.002808094 CEST	53	55570	8.8.8.8	192.168.2.4
Oct 1, 2022 17:09:03.664727926 CEST	64906	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:09:03.688505888 CEST	53	64906	8.8.8.8	192.168.2.4
Oct 1, 2022 17:09:12.428196907 CEST	59446	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:09:12.447535038 CEST	53	59446	8.8.8.8	192.168.2.4
Oct 1, 2022 17:09:18.868763924 CEST	50861	53	192.168.2.4	8.8.8.8
Oct 1, 2022 17:09:18.888529062 CEST	53	50861	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 1, 2022 17:07:14.158483982 CEST	192.168.2.4	8.8.8.8	0xec05	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:20.279519081 CEST	192.168.2.4	8.8.8.8	0xbeb2	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:26.781613111 CEST	192.168.2.4	8.8.8.8	0x5172	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:33.757738113 CEST	192.168.2.4	8.8.8.8	0x7d25	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:40.021703005 CEST	192.168.2.4	8.8.8.8	0x4e43	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Oct 1, 2022 17:07:46.452584028 CEST	192.168.2.4	8.8.8.8	0x2306	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:52.770283937 CEST	192.168.2.4	8.8.8.8	0x8992	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:58.805419922 CEST	192.168.2.4	8.8.8.8	0xdc	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:04.847346067 CEST	192.168.2.4	8.8.8.8	0x3d28	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:11.204330921 CEST	192.168.2.4	8.8.8.8	0xec95	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:17.174144030 CEST	192.168.2.4	8.8.8.8	0x96f1	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:23.640496969 CEST	192.168.2.4	8.8.8.8	0xe397	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:29.868820906 CEST	192.168.2.4	8.8.8.8	0x76bc	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:36.457030058 CEST	192.168.2.4	8.8.8.8	0xb2d7	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:43.453597069 CEST	192.168.2.4	8.8.8.8	0xd063	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:49.599940062 CEST	192.168.2.4	8.8.8.8	0xf917	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:55.983712912 CEST	192.168.2.4	8.8.8.8	0xdcff	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:09:03.664727926 CEST	192.168.2.4	8.8.8.8	0xd6c3	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:09:12.428196907 CEST	192.168.2.4	8.8.8.8	0x24e4	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:09:18.868763924 CEST	192.168.2.4	8.8.8.8	0xa7a0	Standard query (0)	cable-corporation.at.playit.gg	A (IP address)	IN (0x0001)	false

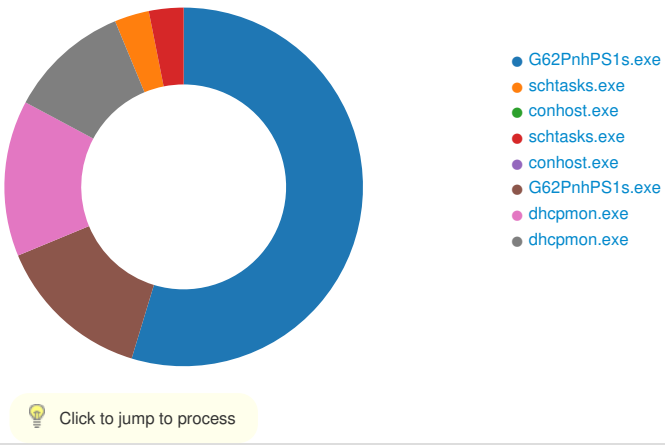
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 1, 2022 17:07:14.183562040 CEST	8.8.8.8	192.168.2.4	0xec05	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:20.387448072 CEST	8.8.8.8	192.168.2.4	0xbeb2	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:26.800611973 CEST	8.8.8.8	192.168.2.4	0x5172	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:33.775125980 CEST	8.8.8.8	192.168.2.4	0x7d25	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:40.041121006 CEST	8.8.8.8	192.168.2.4	0x4e43	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:46.469997883 CEST	8.8.8.8	192.168.2.4	0x2306	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:52.793500900 CEST	8.8.8.8	192.168.2.4	0x8992	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:07:58.824583054 CEST	8.8.8.8	192.168.2.4	0xdc	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Oct 1, 2022 17:08:04.881993055 CEST	8.8.8.8	192.168.2.4	0x3d28	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:11.232418060 CEST	8.8.8.8	192.168.2.4	0xec95	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:17.193731070 CEST	8.8.8.8	192.168.2.4	0x96f1	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:23.669296980 CEST	8.8.8.8	192.168.2.4	0xe397	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:29.888377905 CEST	8.8.8.8	192.168.2.4	0x76bc	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:36.474857092 CEST	8.8.8.8	192.168.2.4	0xb2d7	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:43.482404947 CEST	8.8.8.8	192.168.2.4	0xd063	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:49.623954058 CEST	8.8.8.8	192.168.2.4	0xf917	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:08:56.002808094 CEST	8.8.8.8	192.168.2.4	0xdcff	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:09:03.688505888 CEST	8.8.8.8	192.168.2.4	0xd6c3	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:09:12.447535038 CEST	8.8.8.8	192.168.2.4	0x24e4	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false
Oct 1, 2022 17:09:18.888529062 CEST	8.8.8.8	192.168.2.4	0xa7a0	No error (0)	cable-corporation.at.playit.gg		209.25.141.180	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: G62PnhPS1s.exe PID: **5512**, Parent PID: **3528**

General

Target ID:	0
Start time:	17:07:11
Start date:	01/10/2022
Path:	C:\Users\user\Desktop\G62PnhPS1s.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\G62PnhPS1s.exe
Imagebase:	0x400000
File size:	1246208 bytes
MD5 hash:	07653FD9F64401F9F1696F4782C926F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.579918584.0000000005D60000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.579790309.0000000005AD0000.00000004.10000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.579790309.0000000005AD0000.00000004.10000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000000.00000002.579790309.0000000005AD0000.00000004.10000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.579790309.0000000005AD0000.00000004.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.575419070.00000000031C1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	53B0D15	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	53B0E0F	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	53B0D15	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	53B1094	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	53B1094	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF33C.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	53B1290	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	53B0E0F	CreateFileW
C:\Users\user\AppData\Local\Temp\tmpF531.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	53B1290	GetTempFileNameW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	53B0D15	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	53B0D15	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF33C.tmp	success or wait	1	286BF0E	DeleteFileW
C:\Users\user\AppData\Local\Temp\tmpF531.tmp	success or wait	1	286BF0E	DeleteFileW
C:\Users\user\Desktop\G62PnhPS1s.exe:Zone.Identifier	success or wait	1	53B1625	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	22 59 fd fd fd fd 48	YH	success or wait	1	53B0FC7	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 06 00 fd 27 fd 54 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 08 00 00 48 01 00 00 62 01 00 00 00 00 00 3c fd 00 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 40 39 00 00 04 00 00 00 00 00 00 02 00 00 00 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL'THb< @ @9	success or wait	5	53B1094	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	53B1094	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF33C.tmp	0	1300	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	53B0FC7	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	0	37	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 47 36 32 50 6e 68 50 53 31 73 2e 65 78 65	C:\Users\user\Desktop\G62PnhPS1s.exe	success or wait	1	53B0FC7	WriteFile
C:\Users\user\AppData\Local\Temp\tmpF531.tmp	0	1310	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 20 2f 3e 0d 0a 20 20 3c 54 72 69 67 67 65 72 73 20 2f 3e 0d 0a 20 20 3c 50 72 69 6e 63 69 70 61 6c 73 3e 0d 0a 20 20 20 20 3c 50 72 69 6e 63 69 70 61 6c 20 69 64 3d 22 41 75 74 68 6f 72 22 3e 0d 0a 20 20 20 20 20 20 3c 4c 6f 67 6f 6e 54 79 70 65 3e 49 6e 74 65 72 61 63 74 69 76 65 54 6f 6b 65 6e 3c 2f 4c 6f 67 6f 6e 54 79 70 65 3e	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo /> <Triggers /> <Principals> <Principal id="Author"> <LogonType>InteractiveToken</LogonType>	success or wait	1	53B0FC7	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\G62PnhPS1s.exe	unknown	64	success or wait	1	487706	NtReadFile
C:\Users\user\Desktop\G62PnhPS1s.exe	unknown	20	success or wait	1	487706	NtReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	5B400E	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	72F0BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	72F0BF06	unknown
C:\Users\user\Desktop\G62PnhPS1s.exe	unknown	4096	success or wait	1	72F0BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	53B0FC7	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	53B1186	RegSetValueExW

Analysis Process: schtasks.exe PID: **5552**, Parent PID: **5512**

General

Target ID:	1
Start time:	17:07:12
Start date:	01/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmpF33C.tmp
Imagebase:	0x1f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF33C.tmp	unknown	2	success or wait	1	1FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF33C.tmp	unknown	1301	success or wait	1	1FABD9	ReadFile

Analysis Process: conhost.exe PID: **5560**, Parent PID: **5552**

General

Target ID:	2
Start time:	17:07:12
Start date:	01/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000

File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: **5604**, Parent PID: **5512**

General

Target ID:	3
Start time:	17:07:13
Start date:	01/10/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmpF531.tmp
Imagebase:	0x1f0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF531.tmp	unknown	2	success or wait	1	1FAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF531.tmp	unknown	1311	success or wait	1	1FABD9	ReadFile

Analysis Process: conhost.exe PID: **5612**, Parent PID: **5604**

General

Target ID:	4
Start time:	17:07:13
Start date:	01/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: G62PnhPS1s.exe PID: **5688**, Parent PID: **1088**

General

Target ID:	5
Start time:	17:07:14
Start date:	01/10/2022

Path:	C:\Users\user\Desktop\G62PnhPS1s.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\G62PnhPS1s.exe 0
Imagebase:	0x400000
File size:	1246208 bytes
MD5 hash:	07653FD9F64401F9F1696F4782C926F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000002.329900820.00000000042C6000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000005.00000002.324622791.0000000000402000.00000040.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.324622791.0000000000402000.00000040.00000001.01000000.00000003.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000002.324622791.0000000000402000.00000040.00000001.01000000.00000003.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000005.00000002.329067555.0000000003251000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000005.00000002.329067555.0000000003251000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\G62PnhPS1s.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4F48B3	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\G62PnhPS1s.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	7310A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\G62PnhPS1s.exe	unknown	64	success or wait	1	487706	NtReadFile
C:\Users\user\Desktop\G62PnhPS1s.exe	unknown	20	success or wait	1	487706	NtReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile

Analysis Process: dhcpmon.exe PID: **5708**, Parent PID: **1088**

General

Target ID:	6
Start time:	17:07:14
Start date:	01/10/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x400000
File size:	1246208 bytes
MD5 hash:	07653FD9F64401F9F1696F4782C926F4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.329734424.000000000422E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.329633274.0000000004219000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000006.00000002.329073054.00000000031D1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000006.00000002.329073054.00000000031D1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: SUSP_XORed_URL_in_EXE, Description: Detects an XORed URL in an executable, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 85%, ReversingLabs • Detection: 51%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	4F48B3	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	0	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",03,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",03,"	success or wait	1	7310A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	64	success or wait	1	487706	NtReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	20	success or wait	1	487706	NtReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile

Analysis Process: dhcpmon.exe PID: **5816**, Parent PID: **3528**

General

Target ID:	7
Start time:	17:07:24
Start date:	01/10/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x400000
File size:	1246208 bytes
MD5 hash:	07653FD9F64401F9F1696F4782C926F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E360AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	64	success or wait	1	487706	NtReadFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	unknown	20	success or wait	1	487706	NtReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	5B400E	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	5B400E	ReadFile

Disassembly

No disassembly