ID: 798888
Sample Name:
WmtuqNHPM2.exe
Cookbook: default.jbs
Time: 22:11:09
Date: 05/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

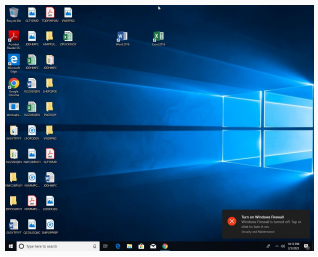
Windows Analysis Report

WmtuqNHPM2.exe

Overview

General Information

Sample Name:	WmtuqNHPM2.exe
Analysis ID:	798888
MD5:	bbe4ba566d22…
SHA1:	ffb73821d698b…
SHA256:	aeb8e080b996…
Tags:	exe NanoCore RAT
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

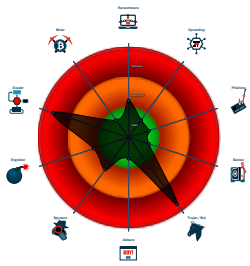
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Antivirus / Scanner detection for sub…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Tries to detect sandboxes and other…
- Yara detected Costura Assembly Lo…

Classification



Process Tree

- **System is w10x64**
- WmtuqNHPM2.exe (PID: 4748 cmdline: C:\Users\user\Desktop\WmtuqNHPM2.exe MD5: BBE4BA566D229A405DA3AF72193D297F)
  - powershell.exe (PID: 1224 cmdline: "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA== MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 1312 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WmtuqNHPM2.exe (PID: 1804 cmdline: C:\Users\user\Desktop\WmtuqNHPM2.exe MD5: BBE4BA566D229A405DA3AF72193D297F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "19b525d2-02f6-47c5-b606-1d038212",
  "Group": "Set",
  "Domain1": "rcontrol4sec.ddnsgeek.com",
  "Domain2": "127.0.0.1",
  "Port": 5080,
  "KeyboardLogging": "Enable",
  "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

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.573280284.0000000003BE1000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x27b0b:$a1: NanoCore.ClientPluginHost • 0x27ae2:$a2: NanoCore.ClientPlugin • 0x2cb36:$b7: LogClientException • 0x27af8:$b9: IClientLoggingHost
00000003.00000002.576770822.0000000005380000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x8ba5:$x1: NanoCore.ClientPluginHost • 0x8bd2:$x2: IClientNetworkHost
00000003.00000002.576770822.0000000005380000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x8ba5:$x2: NanoCore.ClientPluginHost • 0x9b74:$s2: FileCommand • 0xe576:$s4: PipeCreated • 0x8bbf:$s5: IClientLoggingHost
00000003.00000002.576770822.0000000005380000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x8b7f:$x2: NanoCore.ClientPlugin • 0x8ba5:$x3: NanoCore.ClientPluginHost • 0x8b70:$i3: IClientNetwork • 0x8b95:$i5: IClientDataHost • 0x8bbf:$i6: IClientLoggingHost • 0x8bd2:$i7: IClientNetworkHost • 0x8be5:$i9: IClientNameObjectCollection • 0x8902:$s1: ClientPlugin • 0x8b88:$s1: ClientPlugin
00000003.00000002.576770822.0000000005380000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x8ba5:$a1: NanoCore.ClientPluginHost • 0x8b7f:$a2: NanoCore.ClientPlugin • 0x8bbf:$b9: IClientLoggingHost
Click to see the 100 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.WmtuqNHPM2.exe.6d80000.29.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x5b99:$x1: NanoCore.ClientPluginHost • 0x5bb3:$x2: IClientNetworkHost
3.2.WmtuqNHPM2.exe.6d80000.29.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x5b99:$x2: NanoCore.ClientPluginHost • 0x6bce:$s4: PipeCreated • 0x5b86:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
3.2.WmtuqNHPM2.exe.6d80000.29.raw.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x5b70:$x2: NanoCore.ClientPlugin • 0x5b99:$x3: NanoCore.ClientPluginHost • 0x5b61:$i3: IClientNetwork • 0x5b86:$i6: IClientLoggingHost • 0x5bb3:$i7: IClientNetworkHost • 0x59d4:$s1: ClientPlugin • 0x5b79:$s1: ClientPlugin • 0x5e84:$s2: EndPoint • 0x5e8d:$s3: IPAddress • 0x5e97:$s4: IPEndPoint
3.2.WmtuqNHPM2.exe.6d80000.29.raw.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x5b99:$a1: NanoCore.ClientPluginHost • 0x5b70:$a2: NanoCore.ClientPlugin • 0x5b86:$b9: IClientLoggingHost
3.2.WmtuqNHPM2.exe.5640000.24.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x605:$x1: NanoCore.ClientPluginHost • 0x63e:$x2: IClientNetworkHost
Click to see the 279 entries				

Sigma Signatures

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Snort Signatures

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8

Timestamp:	192.168.2.48.8.8.858565532834936 02/05/23-22:13:01.009276
SID:	2834936
Source Port:	58565
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236

Timestamp:	192.168.2.4185.81.157.2364969650802025019 02/05/23-22:12:42.607812
SID:	2025019
Source Port:	49696
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236

Timestamp:	192.168.2.4185.81.157.2364969850802816766 02/05/23-22:12:55.969019
SID:	2816766
Source Port:	49698

Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.852239532834936 02/05/23-22:13:07.004800
SID:	2834936
Source Port:	52239
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.859683532834936 02/05/23-22:12:48.706302
SID:	2834936
Source Port:	59683
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970250802816766 02/05/23-22:13:21.381361
SID:	2816766
Source Port:	49702
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.855570532834936 02/05/23-22:13:46.917410
SID:	2834936
Source Port:	55570
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970350802025019 02/05/23-22:13:26.785835
SID:	2025019
Source Port:	49703
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970750802025019 02/05/23-22:13:53.371030
SID:	2025019
Source Port:	49707
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970850802816766 02/05/23-22:14:01.617464
SID:	2816766
Source Port:	49708
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364969550802816766 02/05/23-22:12:36.467761
SID:	2816766
Source Port:	49695
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.856807532834936 02/05/23-22:13:13.564883
SID:	2834936
Source Port:	56807
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.859446532834936 02/05/23-22:14:00.808827
SID:	2834936
Source Port:	59446
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970850802025019 02/05/23-22:14:01.155093
SID:	2025019
Source Port:	49708
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.860686532834936 02/05/23-22:13:26.675466
SID:	2834936
Source Port:	60686
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970150802025019 02/05/23-22:13:13.802670
SID:	2025019
Source Port:	49701
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364969550802025019 02/05/23-22:12:34.327373
SID:	2025019
Source Port:	49695
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364969950802025019 02/05/23-22:13:01.066179
SID:	2025019
Source Port:	49699

Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keepalive Response 1 - Source IP: 185.81.157.236 - Destination IP: 192.168.2.4	−
Timestamp:	185.81.157.236192.168.2.45080496982810290 02/05/23-22:12:55.383837
SID:	2810290
Source Port:	5080
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	−
Timestamp:	192.168.2.48.8.8.861124532834936 02/05/23-22:13:33.702804
SID:	2834936
Source Port:	61124
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	−
Timestamp:	192.168.2.4185.81.157.2364970050802025019 02/05/23-22:13:07.182076
SID:	2025019
Source Port:	49700
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	−
Timestamp:	192.168.2.4185.81.157.2364970350802816766 02/05/23-22:13:28.533812
SID:	2816766
Source Port:	49703
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	−
Timestamp:	192.168.2.4185.81.157.2364970150802816718 02/05/23-22:13:14.238501
SID:	2816718
Source Port:	49701
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	−
Timestamp:	192.168.2.4185.81.157.2364970450802025019 02/05/23-22:13:33.759288
SID:	2025019
Source Port:	49704
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	−
Timestamp:	192.168.2.4185.81.157.2364970750802816766 02/05/23-22:13:55.082898
SID:	2816766
Source Port:	49707
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970250802025019 02/05/23-22:13:20.465789
SID:	2025019
Source Port:	49702
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970050802816766 02/05/23-22:13:08.202184
SID:	2816766
Source Port:	49700
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.850911532834936 02/05/23-22:12:42.244175
SID:	2834936
Source Port:	50911
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364969850802025019 02/05/23-22:12:54.927420
SID:	2025019
Source Port:	49698
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364969650802816766 02/05/23-22:12:43.716857
SID:	2816766
Source Port:	49696
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.856572532834936 02/05/23-22:12:33.158126
SID:	2834936
Source Port:	56572
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound) - Source IP: 185.81.157.236 - Destination IP: 192.168.2.4	
Timestamp:	185.81.157.236192.168.2.45080496982841753 02/05/23-22:12:59.968145
SID:	2841753
Source Port:	5080
Destination Port:	49698
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364969950802816766 02/05/23-22:13:02.138518
SID:	2816766
Source Port:	49699

Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970550802025019 02/05/23-22:13:40.652150
SID:	2025019
Source Port:	49705
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970450802816766 02/05/23-22:13:34.738607
SID:	2816766
Source Port:	49704
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.861007532834936 02/05/23-22:13:20.247193
SID:	2834936
Source Port:	61007
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970650802816766 02/05/23-22:13:47.957729
SID:	2816766
Source Port:	49706
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970150802816766 02/05/23-22:13:15.190241
SID:	2816766
Source Port:	49701
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364969750802816766 02/05/23-22:12:49.673877
SID:	2816766
Source Port:	49697
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.864906532834936 02/05/23-22:13:53.251157
SID:	2834936
Source Port:	64906
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364969750802025019 02/05/23-22:12:48.883083
SID:	2025019
Source Port:	49697
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.859444532834936 02/05/23-22:13:40.377957
SID:	2834936
Source Port:	59444
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ETPRO TROJAN NanoCore RAT CnC 7 - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970550802816766 02/05/23-22:13:41.829847
SID:	2816766
Source Port:	49705
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com) - Source IP: 192.168.2.4 - Destination IP: 8.8.8.8	
Timestamp:	192.168.2.48.8.8.864167532834936 02/05/23-22:12:54.870549
SID:	2834936
Source Port:	64167
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.4 - Destination IP: 185.81.157.236	
Timestamp:	192.168.2.4185.81.157.2364970650802025019 02/05/23-22:13:46.971431
SID:	2025019
Source Port:	49706
Destination Port:	5080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

Yara detected Costura Assembly Loader

.NET source code contains potential unpacker

Persistence and Installation Behavior

Drops executable to a common third party application directory

Boot Survival

Creates an undocumented autostart registry key

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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

HIPS / PFW / Operating System Protection Evasion

Encrypted powershell cmdline option found

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

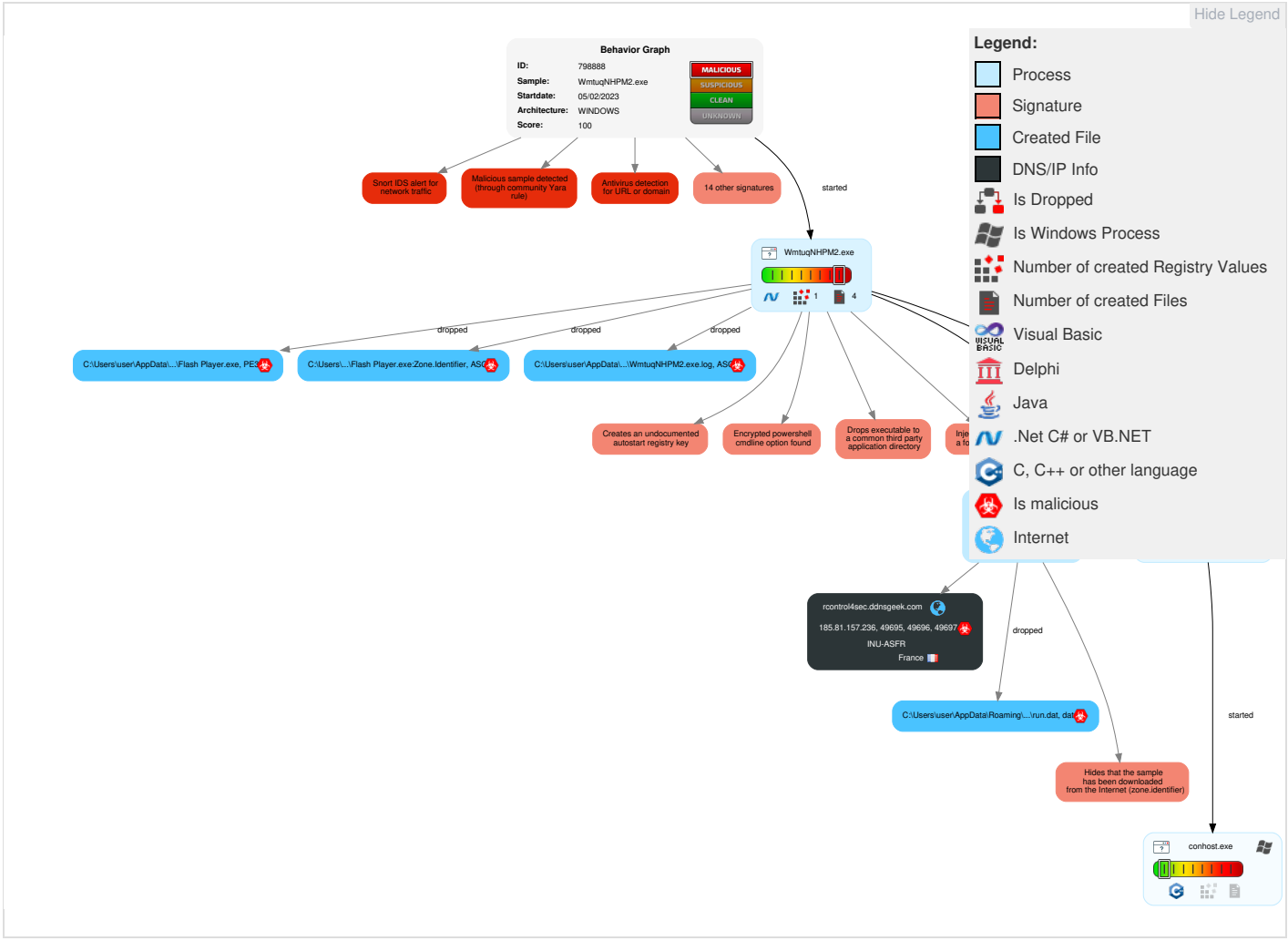
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

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 1 2 Process Injection	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 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 PowerShell	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 1 Deobfuscate/Decode Files or Information	LSASS Memory	1 File and Directory Discovery	Remote Desktop Protocol	1 1 Input Capture	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	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 3 Software Packing	NTDS	2 1 1 Security Software Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Timestomp	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 1 Masquerading	Cached Domain Credentials	2 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	2 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 1 2 Process Injection	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

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

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
WmtuqNHPM2.exe	37%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	
WmtuqNHPM2.exe	46%	Virustotal		Browse
WmtuqNHPM2.exe	100%	Avira	TR/Dropper.MSIL.Gen	
WmtuqNHPM2.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Adobe\Flash Player.exe	100%	Avira	TR/Dropper.MSIL.Gen	
C:\Users\user\AppData\Roaming\Adobe\Flash Player.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\Adobe\Flash Player.exe	45%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	
C:\Users\user\AppData\Roaming\Adobe\Flash Player.exe	46%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.WmtuqNHPM2.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.0.WmtuqNHPM2.exe.d50000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen		Download File
3.2.WmtuqNHPM2.exe.53b0000.19.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

Source	Detection	Scanner	Label	Link
rcontrol4sec.ddnsgeek.com	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://james.newtonking.com/projects/json	0%	URL Reputation	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
rcontrol4sec.ddnsgeek.com	100%	Avira URL Cloud	malware	
rcontrol4sec.ddnsgeek.com	2%	Virustotal		Browse
127.0.0.1	1%	Virustotal		Browse

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
rcontrol4sec.ddnsgeek.com	185.81.157.236	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

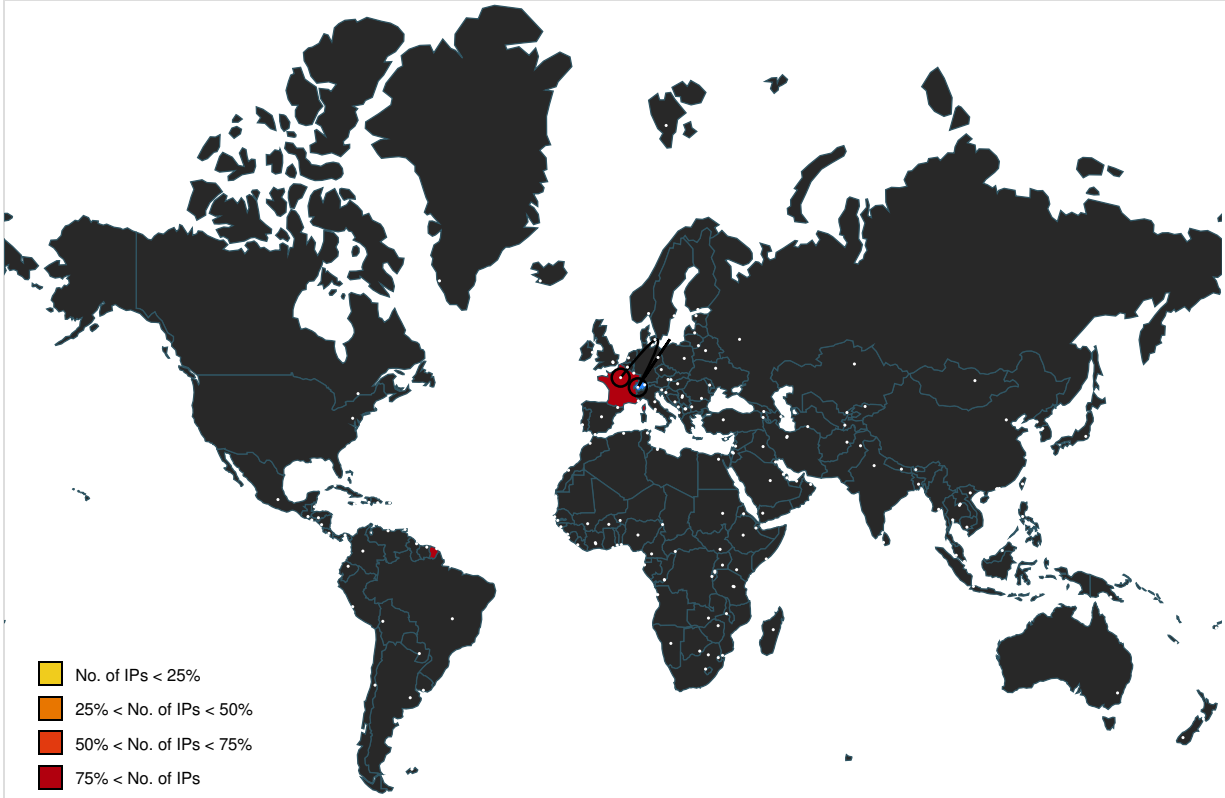
Name	Malicious	Antivirus Detection	Reputation
rcontrol4sec.ddnsgeek.com	true	• 2%, Virustotal, Browse • Avira URL Cloud: malware	unknown
127.0.0.1	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.nuget.org/packages/Newtonsoft.Json.Bson	WmtuqNHPM2.exe, 00000000.00000002.373707879.0000000005800000.00000004.08000000.00040000.00000000.sdmp, WmtuqNHPM2.exe, 00000000.00000002.361584928.000000000442F000.00000004.00000800.00020000.00000000.sdmp, WmtuqNHPM2.exe, 00000000.00000002.361584928.0000000004824000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://api.telegram.org/bot	WmtuqNHPM2.exe, 00000000.00000002.360372340.0000000003223000.00000004.00000800.00020000.00000000.sdmp	false		high
http://google.com	WmtuqNHPM2.exe, 00000003.00000002.573280284.0000000003ED6000.00000004.00000800.00020000.00000000.sdmp, WmtuqNHPM2.exe, 00000003.00000002.567097554.0000000002C5E000.00000004.00000800.00020000.00000000.sdmp, WmtuqNHPM2.exe, 00000003.00000002.579100921.0000000006D50000.00000004.08000000.00040000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	WmtuqNHPM2.exe, 00000003.00000002.567097554.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp	false		high
http://james.newtonking.com/projects/json	WmtuqNHPM2.exe, 00000000.00000002.360372340.0000000003223000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.newtonsoft.com/jsonschema	WmtuqNHPM2.exe, 00000000.00000002.373707879.0000000005800000.00000004.08000000.00040000.00000000.sdmp, WmtuqNHPM2.exe, 00000000.00000002.361584928.000000000442F000.00000004.00000800.00020000.00000000.sdmp, WmtuqNHPM2.exe, 00000000.00000002.361584928.0000000004824000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.81.157.236	rcontrol4sec.ddnsgeek.com	France		198375	INU-ASFR	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	798888
Start date and time:	2023-02-05 22:11:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 57s
Hypervisor based Inspection enabled:	false
Report type:	light
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:	9
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:	WmtuqNHPM2.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@6/11@14/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

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

Simulations

Behavior and APIs

Time	Type	Description
22:12:08	API Interceptor	45x Sleep call for process: powershell.exe modified
22:12:31	API Interceptor	780x Sleep call for process: WmtuqNHPM2.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WmtuqNHPM2.exe.log

Process:	C:\Users\user\Desktop\WmtuqNHPM2.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1039
Entropy (8bit):	5.3436815157474165
Encrypted:	false
SSDEEP:	24:ML9E4Ks2EAE4Kzr7RKDE4KhK3VZ9pKhyE4KdE4KBLWE4Ks:MxHKXEAHKzvRYHKhQnoyHKdHKBqHKs
MD5:	20799406D8EAB97C5485A916A278ED0D
SHA1:	8547571BD0A17ED48FBECDE6D5E4749A66933D53
SHA-256:	BDDBB29FA099BDEB1C409FE844BDA2820D0550E0C97F7A64E01A0EAE4DBDF067
SHA-512:	CA887D0283B3B65BDFA91C90FAAD4C485B3861EEE54C1E6C3A7563DA77DD0D59AC20207259084E2A85E8FC25A48EB805E86904DA60B4C165B03B4A7D758C75 06
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeIma ges_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c5619 34e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..3,"System.Core, Version=4.0. 0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d 16a3b6d\System.Core.ni.dll",0..2,"System.Numerics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Versio n=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad 5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll",0..2,"System.Data, Version=4.0.0.0, Culture=neutra

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	5829
Entropy (8bit):	4.902247628650607
Encrypted:	false
SSDEEP:	96:3CJ2Woe5F2k6Lm5emmXIGegyg12jDs+un/iQLEYFjDaeWJ6KGcmXs9smEFRLcU6j:Wxoe5FVsm5emdzgkjDt4iWN3yBGHc9s8
MD5:	F948233D40FE29A0FFB67F9BB2F050B5
SHA1:	9A815D3F218A9374788F3ECF6BE3445F14B414D8
SHA-256:	C18202AA4EF262432135AFF5139D0981281F528918A2EEA3858B064DFB66BE4F
SHA-512:	FD86A2C713FFA10FC083A34B60D7447DCB0622E83CC5992BBDAB8B3C7FEB7150999A68A8A9B055F263423478C0879ED462B7669FDE7067BC829D79DD3974787 C
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	PSMODULECACHE.....Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ...fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scr ipt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule... .....Find-Module.....Find-RoleCapability.....Publish-Script.....T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1* .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	16592
Entropy (8bit):	5.542066179027588
Encrypted:	false
SSDEEP:	384:gte/Y7sH/gBEZJQlTz+pkLSBxnHgjuVtiJ9gGSJ3uzi13Yv:lfga6L4xHgSVBGcu1v
MD5:	65DBB4F037A4303ADEFFF74F62BC61BB
SHA1:	61ADB67BDE41C4008BD1BF79C5D786CD7777A917
SHA-256:	31B9A26860543E3DD81BB61D069FE78697026BFF2DDBC9E416405018D80C8720
SHA-512:	9E3A4F3F3578F8A318BD1EC8DA983CDE6941EC9E5F4DB0A5A3D47A82D58B70AD13CF1E3C1389BA4B58DB26A85869CB245AF5A64E97CA8D0B3DF45B1D21FC(57D
Malicious:	false
Reputation:	low

Preview:	@...e.....2...:.....@.....H.....<@.^.L."My....'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_mwewao31.inp.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_n31va3q2.xzf.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Adobe\Flash Player.exe

Process:	C:\Users\user\Desktop\WmtuqNHPM2.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1346560
Entropy (8bit):	**7.9984379769425455**
Encrypted:	**true**
SSDEEP:	24576:8ixNAopnJcU4TgHosbIY95AcS1h9VOzYJ0Natxb:8iFpnx4TUosbIYEcSGQ06
MD5:	BBE4BA566D229A405DA3AF72193D297F
SHA1:	FFB73821D698BC2E32F1A32C7ADF95E66520C7A8
SHA-256:	AEB8E080B996A75F85BB82E2E7A42D0302735713F34FB95FFF1BFB97A030E107
SHA-512:	A3BA9225B2719F482F807FE91217CDCCBB9C415D54A8CD4531960BF20456868BA7FB1BE2E473C26F306C33B74615A6F5192F0C852DCA25C66E6D63A4CBB25529
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 45% • Antivirus: Virustotal, Detection: 46%, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....S.....0...../... .....@.. ....`.....@..B.....@.....H.....#..p.....(....*..(....*..0..~.....+q. nq.....%.....(.....s.....s.....s....s.....o.....,...o.....o.....%,.. o.....,..o.....&.....X...2..*..*...4....6..@.....(..V.....".>`.....ej.....*..(...*..0.....r...p.....(.....".....%.....(....%.....(....%..$...(....%..$...(.....(....s.....o.....~....o.....~ ....'... (....r...pr...p.(!.....".....%.....(.....("....o#....~$...o

C:\Users\user\AppData\Roaming\Adobe\Flash Player.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\WmtuqNHPM2.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**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\WmtuqNHPM2.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7r3l3TmKEt5mT1DhFtMhXvvHOxHB3GDq:X4LEnybgCFCtvd7bl3ThE4T19FtMhXvs
MD5:	061E700FE27D852034A5A44BF5985CCF
SHA1:	15B072DE6D6FDD92AE36F074345FA41985833E8D
SHA-256:	4BBB88AF530693EB4A710B0591D4BAF585837242C5690F5A821BF2FC9CC587CD
SHA-512:	CF6C5458AB50C859740490985D1E7E887D1116F3FA947FF2EC49AF9997A42F3402C63EF42B93498544195D9859FBB19CCC295966564B30F5ADB4A36D4E8886C6
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....f.Z#.|...@HkG....G..O*V.....pz...."....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L...A.t...F.{....C.|&.w

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\WmtuqNHPM2.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:v6:y
MD5:	964A446FF1715498B235D5D011A2109D
SHA1:	B1D766A26CFFE4C9893B99A117416019832808CE
SHA-256:	802FDDABB05B022050C084069665F1055AF2516F320B85D3429DA1A2727EF48E
SHA-512:	F87AF7D409E0FCADD24AA454F013707381A4AE0A71770944CA3DF734C8E573E4055685C0005030B60D796E05915D08216AD93B500C7AB102923567A6178DB9D7
Malicious:	**true**
Preview:	.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\WmtuqNHPM2.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48

SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

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

Process:	C:\Users\user\Desktop\WmtuqNHPM2.exe
File Type:	data
Category:	dropped
Size (bytes):	329840
Entropy (8bit):	**7.999431858086539**
Encrypted:	**true**
SSDEEP:	6144:2JUYKN0AL336OXchpvDZhPsrBmnKF/CMnFWxayceW6wElU16sY8:SxKN0S6OshPKrBTF/C9cycepwE3b8
MD5:	9288D88823EFAAD00763F5F9128459FF
SHA1:	78BDD07D4B419E49DCCC3924A41AD92E3B397B23
SHA-256:	5A7678C34A7502234C3151E49D68917F3C68CB83087A5ED9EA8829183D51FBAD
SHA-512:	2A7204479E453A4857A10870A450783C548CD784AB3EA29516B8FF4816EF30841346C4CE3B2ABCD3C24410AFE71903B3C632C408B05FF4F5A2DBCD78A167C35
Malicious:	false
Preview:	.A.<.-.K.....59.. b.FDn..J.y...#.;).x#.4...$..h.a.N.2m....uG..]7.....JTv..1..'.Ke.R..z...%!.1.Wo%.%....u..xdCy!d+....|Y..k.(....XL.../Z..W'.....1o._40.....f.ii6[..g.j@m+..{:&).N...+l{ .hQ+.....(FF._.Y.u.....I...U..J..EA.5k...(.....L...qB#e.[.2P:B.W.r..;...KV)Yj....{..N.....R.z.t/.K..A....G.wkZ..&(....r.)..zt..?kK.$3&B!f.=.4..^..3...~..u.+%....n.RV.n....[.&..... n.....v.,...]).<a.D)....>%./.*..O0...C...b.UI.>....h..8.....I..Fm.G5K....4H.....,3....0zf.....[.../.....".c...-.7F).bXq..$7...C...OT.M.u.....,3.,.....v..-..G.....N....wf0!..... ."..:.(..,?. S...<F$.]..2.....n..IV[....k...x)E._.../x...'6.f...Z\....:.X..}...t..R.m...I. .s.....T.q....."t<.!....s.9..V..*:.....1.b/..x.A....7.>..j~...e...wT.U$O.Y` .R..C...&.-v*.8...:....8..<&R...X...B...w .....c.>...=m.....C.<...K....A....{.....Xdx.X..O2.~.3X..'x.~B..}LD`.@cC.Do.F..P.....!dp...W.....U3.*.V..w..^...\)...:.M...I.K.!.s;.,^.v...c.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.9984379769425455
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	WmtuqNHPM2.exe
File size:	1346560
MD5:	bbe4ba566d229a405da3af72193d297f
SHA1:	ffb73821d698bc2e32f1a32c7adf95e66520c7a8
SHA256:	aeb8e080b996a75f85bb82e2e7a42d0302735713f34fb95fff1bfb97a030e107
SHA512:	a3ba9225b2719f482f807fe91217cdccbb9c415d54a8cd4531960bf20456868ba7fb1be2e473c26f306c33b74615a6f5192f0c852dca25c66e6d63a4cbb25529
SSDEEP:	24576:8ixNAopnJcU4TgHosbIY95AcS1h9VOzYJ0Natxb:8iFpnx4TUosbIYEcSGQ06
TLSH:	7455332539A0AD74E234847C892BF74C2561F101F984A88FE49FD7EBCD8A78457B392D
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....S.....0...../... .....@.. .....`.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x402fe6
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE

DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0xB1B15392 [Fri Jun 20 11:54:58 2064 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview
Instruction
jmp dword ptr [00402000h]
pop ds
mov ecx, dword ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax+eax], al
fdiv st(5), st(0)
pop es
jl 00007F60551507B6h
lds edi, edi
aas
mov gs, di
out dx, al
pop ebp
test dword ptr [eax], edx
mov dl, 49h
dec eax
inc edx
jmp far EB05h : 00F394A2h
fiadd word ptr [ecx+161B0580h]
push esp
aam 60h
and eax, 12091748h
inc eax
movsb
lodsb
pop eax
mov cl, 00h
bound edx, dword ptr [edi+44h]
inc esp
adc al, 15h
inc ebp
inc eax
inc ecx
lds eax, fword ptr [esi+11h]
mov al, 8Bh
fcomp dword ptr [ebx]
mov cl, F7h
div byte ptr [esi-068D2D60h]
int F3h
xor eax, 9BB33BBBh
mov ebp, CFDF2C10h
push ecx
out C1h, eax
in eax, E6h
cmpsw

Instruction
mov esp, 79AF35E6h
mov ebp, BD7AF35Eh
out B8h, al
shl dword ptr [edi+2Bh], cl
and dword ptr [ebp+51h], eax
retn D3ECh
shl byte ptr [eax-01EAD4D8h], 1
scasd
mov bh, B2h
jmp 00007F6055150821h
rcr eax, cl
daa
cmpsd
test eax, E645651Ch
imul ebp, dword ptr [ebp+57h], AAh

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x2f94	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14c000	0x56c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x14e000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x2f78	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x14815c	0x148200	False	0.9945498511904762	data	7.998830102245729	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0x14c000	0x56c	0x600	False	0.4010416666666667	data	3.94255191885509	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x14e000	0xc	0x200	False	0.044921875	data	0.08153941234324169	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x14c090	0x2dc	data		
RT_MANIFEST	0x14c37c	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.48.8.8.8585655 32834936 02/05/23-22:13:01.009276	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	58565	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64969650802025019 02/05/23-22:12:42.607812	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49696	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64969850802816766 02/05/23-22:12:55.969019	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49698	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8522395 32834936 02/05/23-22:13:07.004800	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	52239	53	192.168.2.4	8.8.8.8
192.168.2.48.8.8.8596835 32834936 02/05/23-22:12:48.706302	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	59683	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64970250802816766 02/05/23-22:13:21.381361	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49702	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8555705 32834936 02/05/23-22:13:46.917410	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	55570	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64970350802025019 02/05/23-22:13:26.785835	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970750802025019 02/05/23-22:13:53.371030	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970850802816766 02/05/23-22:14:01.617464	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49708	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64969550802816766 02/05/23-22:12:36.467761	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49695	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8568075 32834936 02/05/23-22:13:13.564883	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	56807	53	192.168.2.4	8.8.8.8
192.168.2.48.8.8.8594465 32834936 02/05/23-22:14:00.808827	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	59446	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64970850802025019 02/05/23-22:14:01.155093	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49708	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8606865 32834936 02/05/23-22:13:26.675466	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	60686	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64970150802025019 02/05/23-22:13:13.802670	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64969550802025019 02/05/23-22:12:34.327373	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49695	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64969950802025019 02/05/23-22:13:01.066179	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49699	5080	192.168.2.4	185.81.157.236
185.81.157.236192.168.2.45080496982810290 02/05/23-22:12:55.383837	TCP	2810290	ETPRO TROJAN NanoCore RAT Keepalive Response 1	5080	49698	185.81.157.236	192.168.2.4
192.168.2.48.8.8.8611245 32834936 02/05/23-22:13:33.702804	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	61124	53	192.168.2.4	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4185.81.157.23 64970050802025019 02/05/23-22:13:07.182076	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970350802816766 02/05/23-22:13:28.533812	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49703	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970150802816718 02/05/23-22:13:14.238501	TCP	2816718	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon	49701	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970450802025019 02/05/23-22:13:33.759288	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970750802816766 02/05/23-22:13:55.082898	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49707	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970250802025019 02/05/23-22:13:20.465789	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970050802816766 02/05/23-22:13:08.202184	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49700	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8509115 32834936 02/05/23-22:12:42.244175	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	50911	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64969850802025019 02/05/23-22:12:54.927420	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64969650802816766 02/05/23-22:12:43.716857	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49696	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8565725 32834936 02/05/23-22:12:33.158126	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	56572	53	192.168.2.4	8.8.8.8
185.81.157.236192.168.2.45080496982841753 02/05/23-22:12:59.968145	TCP	2841753	ETPRO TROJAN NanoCore RAT Keep-Alive Beacon (Inbound)	5080	49698	185.81.157.236	192.168.2.4
192.168.2.4185.81.157.23 64969950802816766 02/05/23-22:13:02.138518	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49699	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970550802025019 02/05/23-22:13:40.652150	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970450802816766 02/05/23-22:13:34.738607	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49704	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8610075 32834936 02/05/23-22:13:20.247193	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	61007	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64970650802816766 02/05/23-22:13:47.957729	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49706	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64970150802816766 02/05/23-22:13:15.190241	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49701	5080	192.168.2.4	185.81.157.236
192.168.2.4185.81.157.23 64969750802816766 02/05/23-22:12:49.673877	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49697	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8649065 32834936 02/05/23-22:13:53.251157	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	64906	53	192.168.2.4	8.8.8.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4185.81.157.23 64969750802025019 02/05/23-22:12:48.883083	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49697	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8594445 32834936 02/05/23-22:13:40.377957	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	59444	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64970550802816766 02/05/23-22:13:41.829847	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49705	5080	192.168.2.4	185.81.157.236
192.168.2.48.8.8.8641675 32834936 02/05/23-22:12:54.870549	UDP	2834936	ETPRO TROJAN Observed DNS Query to Abused DDNS (ddnsgeek .com)	64167	53	192.168.2.4	8.8.8.8
192.168.2.4185.81.157.23 64970650802025019 02/05/23-22:13:46.971431	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	5080	192.168.2.4	185.81.157.236

Network Port Distribution

Total Packets: 49

- 53 (DNS)
- 5080 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2023 22:12:33.382641077 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:33.415704966 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:33.415920019 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:34.327373028 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:34.364419937 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:34.364609003 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:34.457401037 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:34.476407051 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:34.509838104 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:34.560023069 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.393512964 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.468734980 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.470374107 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.549987078 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.570312977 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.570358992 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.570386887 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.570415020 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.570554018 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.603595972 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.603631973 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.603657961 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.603682041 CET	5080	49695	185.81.157.236	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2023 22:12:35.603708029 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.603729010 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.603734970 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.603729010 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.603763103 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.603791952 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.603792906 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.603843927 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.637763977 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637797117 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637823105 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637846947 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637871027 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637896061 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637922049 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637923002 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.637923002 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.637947083 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637972116 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.637994051 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.637994051 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.637996912 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.638024092 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.638046980 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.638050079 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.638072968 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.638096094 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.638117075 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.638124943 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.638143063 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.638154030 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.638192892 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671045065 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671080112 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671106100 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671139956 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671165943 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671189070 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671216011 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671215057 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671215057 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671241999 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671278000 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671289921 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671289921 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671320915 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671346903 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671370029 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671370983 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671399117 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671413898 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671423912 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671448946 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671466112 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671473980 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671500921 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671534061 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671544075 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671571016 CET	5080	49695	185.81.157.236	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2023 22:12:35.671590090 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671595097 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671622038 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671638012 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671653986 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671679974 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671695948 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671706915 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671734095 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671749115 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671758890 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671783924 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671802998 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671809912 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671837091 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671866894 CET	49695	5080	192.168.2.4	185.81.157.236
Feb 5, 2023 22:12:35.671880960 CET	5080	49695	185.81.157.236	192.168.2.4
Feb 5, 2023 22:12:35.671907902 CET	5080	49695	185.81.157.236	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 5, 2023 22:12:33.158126116 CET	56572	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:12:33.335684061 CET	53	56572	8.8.8.8	192.168.2.4
Feb 5, 2023 22:12:42.244174957 CET	50911	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:12:42.421756983 CET	53	50911	8.8.8.8	192.168.2.4
Feb 5, 2023 22:12:48.706301928 CET	59683	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:12:48.843491077 CET	53	59683	8.8.8.8	192.168.2.4
Feb 5, 2023 22:12:54.870548964 CET	64167	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:12:54.890508890 CET	53	64167	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:01.009275913 CET	58565	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:01.029556036 CET	53	58565	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:07.004800081 CET	52239	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:07.146991968 CET	53	52239	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:13.564882994 CET	56807	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:13.739322901 CET	53	56807	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:20.247193098 CET	61007	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:20.418184996 CET	53	61007	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:26.675466061 CET	60686	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:26.695624113 CET	53	60686	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:33.702804089 CET	61124	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:33.723865032 CET	53	61124	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:40.377957106 CET	59444	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:40.521933079 CET	53	59444	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:46.917409897 CET	55570	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:46.935590982 CET	53	55570	8.8.8.8	192.168.2.4
Feb 5, 2023 22:13:53.251157045 CET	64906	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:13:53.271231890 CET	53	64906	8.8.8.8	192.168.2.4
Feb 5, 2023 22:14:00.808826923 CET	59446	53	192.168.2.4	8.8.8.8
Feb 5, 2023 22:14:00.829329014 CET	53	59446	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
Feb 5, 2023 22:12:33.158126116 CET	192.168.2.4	8.8.8.8	0x6f9c	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:12:42.244174957 CET	192.168.2.4	8.8.8.8	0x455b	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Feb 5, 2023 22:12:48.706301928 CET	192.168.2.4	8.8.8.8	0xcff3	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:12:54.870548964 CET	192.168.2.4	8.8.8.8	0x2599	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:01.009275913 CET	192.168.2.4	8.8.8.8	0xe949	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:07.004800081 CET	192.168.2.4	8.8.8.8	0x3ddb	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:13.564882994 CET	192.168.2.4	8.8.8.8	0xd97b	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:20.247193098 CET	192.168.2.4	8.8.8.8	0x37e1	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:26.675466061 CET	192.168.2.4	8.8.8.8	0x161c	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:33.702804089 CET	192.168.2.4	8.8.8.8	0x611c	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:40.377957106 CET	192.168.2.4	8.8.8.8	0x53ac	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:46.917409897 CET	192.168.2.4	8.8.8.8	0x5b7a	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:53.251157045 CET	192.168.2.4	8.8.8.8	0xc6f	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:14:00.808826923 CET	192.168.2.4	8.8.8.8	0xf7db	Standard query (0)	rcontrol4sec.ddnsgeek.com	A (IP address)	IN (0x0001)	false

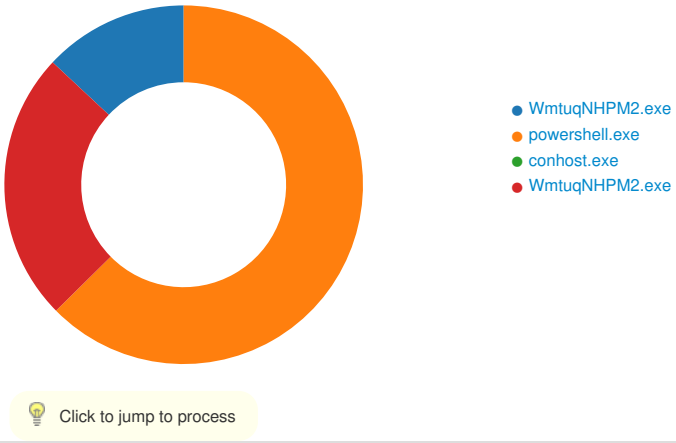
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 5, 2023 22:12:33.335684061 CET	8.8.8.8	192.168.2.4	0x6f9c	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:12:42.421756983 CET	8.8.8.8	192.168.2.4	0x455b	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:12:48.843491077 CET	8.8.8.8	192.168.2.4	0xcff3	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:12:54.890508890 CET	8.8.8.8	192.168.2.4	0x2599	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:01.029556036 CET	8.8.8.8	192.168.2.4	0xe949	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:07.146991968 CET	8.8.8.8	192.168.2.4	0x3ddb	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:13.739322901 CET	8.8.8.8	192.168.2.4	0xd97b	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:20.418184996 CET	8.8.8.8	192.168.2.4	0x37e1	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:26.695624113 CET	8.8.8.8	192.168.2.4	0x161c	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:33.723865032 CET	8.8.8.8	192.168.2.4	0x611c	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:40.521933079 CET	8.8.8.8	192.168.2.4	0x53ac	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Feb 5, 2023 22:13:46.935590982 CET	8.8.8.8	192.168.2.4	0x5b7a	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:13:53.271231890 CET	8.8.8.8	192.168.2.4	0xc6f	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false
Feb 5, 2023 22:14:00.829329014 CET	8.8.8.8	192.168.2.4	0xf7db	No error (0)	rcontrol4sec.ddnsgeek.com		185.81.157.236	A (IP address)	IN (0x0001)	false

Statistics

Behavior



System Behavior

Analysis Process: WmtuqNHPM2.exe PID: 4748, Parent PID: 3528

General

Target ID:	0
Start time:	22:12:00
Start date:	05/02/2023
Path:	C:\Users\user\Desktop\WmtuqNHPM2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\WmtuqNHPM2.exe
Imagebase:	0xd50000
File size:	1346560 bytes
MD5 hash:	BBE4BA566D229A405DA3AF72193D297F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.361584928.000000000420D000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.361584928.000000000420D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.361584928.000000000420D000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.361584928.000000000420D000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.361584928.000000000420D000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.373170392.0000000005690000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: HKTL_NET_NAME_DotNetInject, Description: Detects .NET red/black-team tools via name, Source: 00000000.00000002.373707879.0000000005800000.00000004.08000000.00040000.00000000.sdmp, Author: Arnim Rupp • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.360372340.0000000003223000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000000.00000002.360372340.0000000003223000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.360372340.0000000003223000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.360372340.0000000003223000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.361584928.0000000004390000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.361584928.0000000004390000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.361584928.0000000004390000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.361584928.0000000004390000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.361584928.000000000442F000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.361584928.000000000442F000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.361584928.000000000442F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000000.00000002.361584928.000000000442F000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Adobe\Flash Player.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	5C273C0	CopyFileW
C:\Users\user\AppData\Roaming\Adobe\Flash Player.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	5C273C0	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WmtuqNHPM2.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7312C78D	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\Adobe\Flash Player.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 03 00 fd 53 fd fd 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 14 00 00 08 00 00 00 00 00 00 fd 2f 00 00 00 20 00 00 00 fd 14 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 00 00 15 00 00 02 00 00 00 00 00 00 02 00 60 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELS0/ @ `	success or wait	6	5C273C0	CopyFileW
C:\Users\user\AppData\Roaming\Adobe\Flash Player.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	5C273C0	CopyFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\WmtuqNHPM2.exe.log	0	1039	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 33 32 5c 53 79 73 74 65 6d 5c 34 66 30 61 37 65 65 66 61 33 63 64 33 65 30 62 61 39 38 62 35 65 62 64 64 62 62 63 37 32 65 36 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 58 6d 6c 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e	1,"fusion","GAC",01,"WinRT","NotApp",13,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",03,"System.Xml, Version=4.0.0.	success or wait	1	7312C907	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	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.ni.dll.aux	unknown	1100	success or wait	1	72D503DE	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\Winlogon	Shell	unicode	explorer.exe,"C:\Users\user\AppData\Roaming\Adobe\Flash Player.exe",	success or wait	1	71C6646A	RegSetValueExW

Analysis Process: powershell.exe PID: **1224**, Parent PID: **4748**

General

Target ID:	1
Start time:	22:12:06
Start date:	05/02/2023
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" -ENC cwB0AGEAcgB0AC0AcwBsAGUAZQBwACAALQBzAGUAYwBvAG4AZABzACAAMgAwAA==
Imagebase:	0xbd0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71BC5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	71BC5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_mwewao31.inp.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_n31va3q2.xzf.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72E1CF06	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	72E1CF06	unknown

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mwewao31.inp.ps1	success or wait	1	71C66A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_n31va3q2.xzf.psm1	success or wait	1	71C66A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_mwewao31.inp.ps1	0	1	31	1	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_n31va3q2.xzf.psm1	0	1	31	1	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	0	4096	50 53 4d 4f 44 55 4c 45 43 41 43 48 45 01 07 00 00 00 fd fd fd fd 15 fd fd 08 59 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c 4d 6f 64 75 6c 65 73 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 5c 31 2e 30 2e 30 2e 31 5c 50 6f 77 65 72 53 68 65 6c 6c 47 65 74 2e 70 73 64 31 1d 00 00 00 10 00 00 00 55 6e 69 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 04 00 00 00 69 6e 6d 6f 01 00 00 00 04 00 00 00 66 69 6d 6f 01 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 4d 6f 64 75 6c 65 02 00 00 00 12 00 00 00 4e 65 77 2d 53 63 72 69 70 74 46 69 6c 65 49 6e 66 6f 02 00 00 00 0e 00 00 00 50 75 62 6c 69 73 68 2d 4d 6f 64 75 6c 65 02 00 00 00 0e 00 00 00 49 6e 73 74 61 6c 6c 2d 53 63	PSMODULECACHEYC:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1Uninstall-ModuleinmofimoInstall-ModuleNew-scriptFileInfoPublish-ModuleInstall-Sc	success or wait	1	71C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	4096	1733	00 0a 00 00 00 47 65 74 2d 52 61 6e 64 6f 6d 08 00 00 00 03 00 00 00 43 46 53 01 00 00 00 0a 00 00 00 4f 75 74 2d 53 74 72 69 6e 67 08 00 00 00 0e 00 00 00 57 72 69 74 65 2d 50 72 6f 67 72 65 73 73 08 00 00 00 14 00 00 00 44 69 73 61 62 6c 65 2d 50 53 42 72 65 61 6b 70 6f 69 6e 74 08 00 00 00 11 00 00 00 55 70 64 61 74 65 2d 46 6f 72 6d 61 74 44 61 74 61 08 00 00 00 11 00 00 00 57 72 69 74 65 2d 49 6e 66 6f 72 6d 61 74 69 6f 6e 08 00 00 00 0d 00 00 00 43 6f 6e 76 65 72 74 54 6f 2d 58 6d 6c 08 00 00 00 0c 00 00 00 53 65 74 2d 56 61 72 69 61 62 6c 65 08 00 00 00 0b 00 00 00 4f 75 74 2d 50 72 69 6e 74 65 72 08 00 00 00 fd fd fd fd 79 fd 68 15 fd fd 08 49 00 00 00 43 3a 5c 50 72 6f 67 72 61 6d 20 46 69 6c 65 73 20 28 78 38 36 29 5c 57 69 6e 64 6f 77 73 50	Get-RandomCFSOut-StringWrite-ProgressDisable-PSBreakpointUpdate-FormatDataWrite-InformationConvertTo-XmlSet-VariableOut-PrinteryIC:\Program Files (x86)\WindowsP	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 0f 00 00 00 1e 0f 00 00 13 00 00 00 fd 0e fd 04 0a 0a 02 0a 32 09 00 00 3a 01 fd 00 0e 00 fd 0e 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@e2:@	success or wait	1	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 27 00 00 00 0e 00 20 00	H<@^L"My:'	success or wait	15	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	15	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	730E76FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1004	4	00 08 00 03		success or wait	8	730E76FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1008	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0c fd 00 54 01 40 00 fd 3e 40 01 68 38 40 01 67 38 40 01 10 6f 40 01 11 6f 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 05 0e fd 00 06 0e fd 00 04 0e fd 00 07 0e fd 00 08 0e fd 00 12 6f 40 01 2a 29 40 01 1f 29 40 01 4d 64 40 01 5d 64 40 01 4e 64 40 01 fd 29 40 01 fd 29 40	T@>@h8@g8@o@o@ @V@H@X@[@NT@HT @S @S@hT@S@S@S@\@ T@T@@X@? X@T@S@S@ T@T@xT@zT@T@=M @DM@:M@"M@ M@!M@ ;M@D@D@@M@<M@$ M@8M@? M@o@*)@)@M d@]d@Nd@)@)@	success or wait	8	730E76FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DFCA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	72E01F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	71C61B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	71C61B4F	ReadFile

Analysis Process: conhost.exe PID: **1312**, Parent PID: **1224**

General

Target ID:	2
Start time:	22:12:06
Start date:	05/02/2023
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: WmtuqNHPM2.exe PID: **1804**, Parent PID: **4748**

General

Target ID:	3
Start time:	22:12:29
Start date:	05/02/2023
Path:	C:\Users\user\Desktop\WmtuqNHPM2.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\WmtuqNHPM2.exe
Imagebase:	0x760000
File size:	1346560 bytes
MD5 hash:	BBE4BA566D229A405DA3AF72193D297F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.573280284.0000000003BE1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.576770822.0000000005380000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.576770822.0000000005380000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.576770822.0000000005380000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.576770822.0000000005380000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.576971415.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.576971415.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.576971415.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.576971415.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.576971415.00000000053B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579066865.0000000006D40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579066865.0000000006D40000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579066865.0000000006D40000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579066865.0000000006D40000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579753153.0000000006DF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579753153.0000000006DF0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579753153.0000000006DF0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579753153.0000000006DF0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.573280284.0000000003ED6000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.573280284.0000000003ED6000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.577664511.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.577664511.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.577664511.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.577664511.0000000005640000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579159635.0000000006D60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579159635.0000000006D60000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579159635.0000000006D60000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen

- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579159635.0000000006D60000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579551612.0000000006DC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579551612.0000000006DC0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579551612.0000000006DC0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579551612.0000000006DC0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.573280284.0000000003EBA000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.573280284.0000000003EBA000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.577604617.0000000005630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.577604617.0000000005630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.577604617.0000000005630000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.577604617.0000000005630000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.567097554.0000000002C5E000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.567097554.0000000002C5E000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579206321.0000000006D70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579206321.0000000006D70000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579206321.0000000006D70000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579206321.0000000006D70000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.573280284.0000000003C31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.573280284.0000000003C31000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.576714825.0000000005370000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.576714825.0000000005370000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.576714825.0000000005370000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.576714825.0000000005370000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579100921.0000000006D50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579100921.0000000006D50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579100921.0000000006D50000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579100921.0000000006D50000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.576657661.00000000051E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.576657661.00000000051E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.576657661.00000000051E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.576657661.00000000051E0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579257158.0000000006D80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579257158.0000000006D80000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579257158.0000000006D80000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579257158.0000000006D80000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.577562971.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.577562971.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.577562971.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.577562971.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.563508459.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.563508459.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000003.00000002.563508459.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.563508459.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000003.00000002.579396651.0000000006DA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000003.00000002.579396651.0000000006DA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

	• Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 00000003.00000002.579396651.0000000006DA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.579396651.0000000006DA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000003.00000002.567097554.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000003.00000002.567097554.0000000002BE1000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 00000003.00000002.567097554.0000000002BE1000.00000004.00000800.00020000.00000000.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	72E1CF06	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	72E1CF06	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	71C6BEFF	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	71C61E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	71C6BEFF	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	71C6BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	10	71C61E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	71C61E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WmtuqNHPM2.exe:Zone.Identifier	success or wait	1	71BE2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	fd 16 fd fd fd 07 fd 48	H	success or wait	1	71C61B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	248	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 5f 66 fd 5a 23 fd 7c fd 11 fd 40 48 6b 47 10 1f fd 31 47 fd fd 4f 2a 56 2e 15 0e eb fd 1f fd fd fd fd 70 7a fd fd fd fd 22 fd 0a 07 fd 72 fd fd 10 77 26 26 7c fd fd 63 fd fd 33 7d 7e fd fd fd 1d fd 7e fd f6 fd 6f 73 fd fd 66 fd 05 fd 12 fd fd fd 34 12 fd 31 fd 67 4a fd 27 fd 64 22 fd 4c fd 0b fd 41 fd 74 fd c7 fd 46 fd 7b fd 2b 14 fd 43 0c 7c 26 fd 77	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLfZ#| @HkGGO*V.p z"rw&&|c3}~~osf41gJ'd"L AtF{C|&w	success or wait	14	71C61B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	329840	fd 41 fd 3c fd 2d fd 4b fd 5a fd 1d fd fd 35 39 0a fd 20 62 fd 46 44 6e fd 03 4a fd 79 fd 0b fd 23 fd 3b 29 1f 78 23 fd 34 1c fd fd 24 fd fd 68 fd 61 15 4e 8a 32 6d fd fd d3 fd 75 47 fd 11 5d 37 fd 8c fd fd fd fd fd fd 4a 54 76 fd fd 31 fd fd 27 fd 4b 65 12 52 fd 7f 7a fd fd 1e 25 21 fd 31 fd 57 6f 25 fd 25 fd fd fd fd 75 fd fd 78 64 43 79 21 64 2b fd 0a fd fd 7c 59 fd 05 6b 0f 28 fd fd fd fd 58 4c fd fd 1d 2f 5a 17 fd 57 27 fd fd fd fd 0d fd 31 6f fd 5f 34 30 fd 08 4f fd 1a fd fc 66 fd 69 69 36 5b fd fd 67 fd 6a 40 6d 2b 15 fd 7b 3a 26 29 fd 4e fd fd fd 2b 6c 7b fd 68 51 2b fd 0b fd fd 7f fd 04 28 46 46 fd 5f fd 59 fd 75 12 fd fd fd fd 6c 10 fd 01 55 fd fd 4a fd fd 45 41 fd 35 6b 15 07 0d 28 fd fd 16 fd fd fd fd 4c	A<-K59 bFDnJy#;)x#4$haN2muG]7J Tv1'KeRz%!1Wo%%uxd Cy!d+|Yk(XL/ ZW'1o_40fii6[gj@m+ {:&)N+I{hQ+(FF_YulUJEA5k(L	success or wait	1	71C61B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	71C61B4F	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	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72DF5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DFCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	72D503DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	72D503DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72DF5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	71C61B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	71C61B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\WmtuqNHPM2.exe	unknown	4096	success or wait	1	72DDD72F	unknown
C:\Users\user\Desktop\WmtuqNHPM2.exe	unknown	512	success or wait	1	72DDD72F	unknown

Disassembly

No disassembly