ID: 831164
Sample Name:
Products_inquiry.exe
Cookbook: default.jbs
Time: 07:21:11
Date: 21/03/2023
Version: 37.0.0 Beryl

Table of Contents

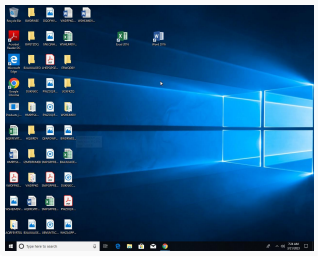
Windows Analysis Report

Products_inquiry.exe

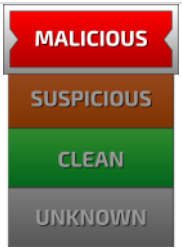
Overview

General Information

Sample Name:	Products_inquiry.exe
Analysis ID:	831164
MD5:	b4ef6d5785dd9..
SHA1:	02c89f672fe72…
SHA256:	0fed79a59d322..
Tags:	exe NanoCore RAT
Infos:	



Detection



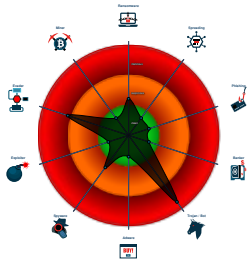
Nanocore

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Snort IDS alert for network traffic
- Machine Learning detection for sam…
- Machine Learning detection for drop…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- Products_inquiry.exe (PID: 5568 cmdline: C:\Users\user\Desktop\Products_inquiry.exe MD5: B4EF6D5785DD94BD5BCE5B980BBFEE62)
  - Products_inquiry.exe (PID: 4124 cmdline: C:\Users\user\Desktop\Products_inquiry.exe MD5: B4EF6D5785DD94BD5BCE5B980BBFEE62)
- dhcpmon.exe (PID: 2008 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: B4EF6D5785DD94BD5BCE5B980BBFEE62)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
Nanocore RAT, NanoCore	Nanocore is a Remote Access Tool used to steal credentials and to spy on cameras. It as been used for a while by numerous criminal actors as well as by nation state threat actors.	• APT33 • The Gorgon Group	**http://** https://assets.virustotal.com/reports/2021trends.pdfhttps://blog.360totalsecurity.com/en/bayworld-event-cyber-attack-against-foreign-trade-industry/https://blog.360totalsecurity.com/en/vendetta-new-threat-actor-from-europe/https://blog.morphisec.com/syk-crypter-discordhttps://blog.talosintelligence.com/2020/02/coronavirus-themed-malware.html	**http://** https://malpedia.caad.fkie.fraunhofer.de/details/win.nanocore

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "a8891f33-1dde-4fa2-97d1-3d63005c",
  "Group": "Default",
  "Domain1": "stevewells.hopto.org",
  "Domain2": "stevewells.hopto.org",
  "Port": 40001,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "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
0000000A.00000002.538870031.00000000040F1000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x27b0b:$a1: NanoCore.ClientPluginHost • 0x27ae2:$a2: NanoCore.ClientPlugin • 0x2cb36:$b7: LogClientException • 0x27af8:$b9: IClientLoggingHost
0000000A.00000002.550430211.0000000006800000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x4bbb:$x1: NanoCore.ClientPluginHost • 0x4be5:$x2: IClientNetworkHost
0000000A.00000002.550430211.0000000006800000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x4bbb:$x2: NanoCore.ClientPluginHost • 0x6a6b:$s4: PipeCreated
0000000A.00000002.550430211.0000000006800000.00000004.08000000.00040000.00000000.sdmp	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x4b96:$x2: NanoCore.ClientPlugin • 0x4bbb:$x3: NanoCore.ClientPluginHost • 0x4b87:$i3: IClientNetwork • 0x4bac:$i4: IClientAppHost • 0x4bd5:$i5: IClientDataHost • 0x4be5:$i7: IClientNetworkHost • 0x4bf8:$i9: IClientNameObjectCollection • 0x4c1d:$i10: IClientReadOnlyNameObjectCollection • 0x49ce:$s1: ClientPlugin • 0x4b9f:$s1: ClientPlugin
0000000A.00000002.550430211.0000000006800000.00000004.08000000.00040000.00000000.sdmp	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x4bbb:$a1: NanoCore.ClientPluginHost • 0x4b96:$a2: NanoCore.ClientPlugin • 0x8558:$b1: get_BuilderSettings • 0x4bac:$b4: IClientAppHost
Click to see the 71 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
10.2.Products_inquiry.exe.7460000.21.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0x6da5:$x1: NanoCore.ClientPluginHost • 0x6dd2:$x2: IClientNetworkHost
10.2.Products_inquiry.exe.7460000.21.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth (Nextron Systems)	• 0x6da5:$x2: NanoCore.ClientPluginHost • 0x7d74:$s2: FileCommand • 0xc776:$s4: PipeCreated • 0x6dbf:$s5: IClientLoggingHost

Source	Rule	Description	Author	Strings
10.2.Products_inquiry.exe.7460000.21.unpack	MALWARE_Win_NanoCore	Detects NanoCore	ditekSHen	• 0x6d7f:$x2: NanoCore.ClientPlugin • 0x6da5:$x3: NanoCore.ClientPluginHost • 0x6d70:$i3: IClientNetwork • 0x6d95:$i5: IClientDataHost • 0x6dbf:$i6: IClientLoggingHost • 0x6dd2:$i7: IClientNetworkHost • 0x6de5:$i9: IClientNameObjectCollection • 0x6b02:$s1: ClientPlugin • 0x6d88:$s1: ClientPlugin
10.2.Products_inquiry.exe.7460000.21.unpack	Windows_Trojan_Nanocore_d8c4e3c5	unknown	unknown	• 0x6da5:$a1: NanoCore.ClientPluginHost • 0x6d7f:$a2: NanoCore.ClientPlugin • 0x6dbf:$b9: IClientLoggingHost
10.2.Products_inquiry.exe.5ba0000.16.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth (Nextron Systems)	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 219 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 NanoCore RAT CnC 7 - Source IP: 192.168.2.3 - Destination IP: 209.182.100.23 −

Timestamp:	192.168.2.3209.182.100.234969740001281676 6 03/21/23-07:23:30.034206
SID:	2816766
Source Port:	49697
Destination Port:	40001
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN Possible NanoCore C2 60B - Source IP: 192.168.2.3 - Destination IP: 209.182.100.23 −

Timestamp:	192.168.2.3209.182.100.234969740001202501 9 03/21/23-07:23:28.411292
SID:	2025019
Source Port:	49697
Destination Port:	40001
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Hooking and other Techniques for Hiding and Protection

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

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

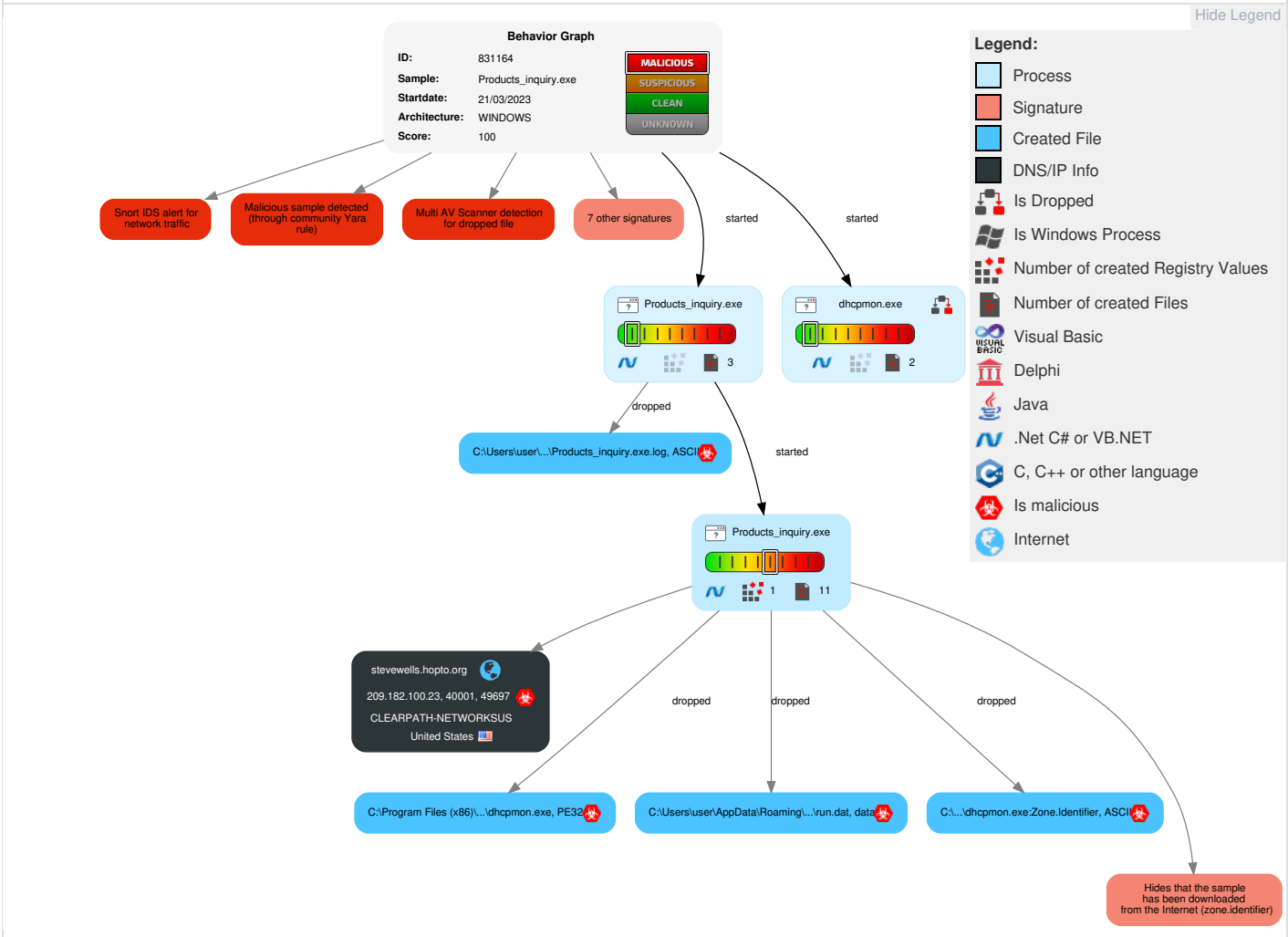
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	Windows Management Instrumentation	Path Interception	1 2 Process Injection	2 Masquerading	1 1 Input Capture	1 Security Software Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Hidden Files and Directories	LSA Secrets	1 2 System Information 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	2 Obfuscated Files or Information	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	3 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

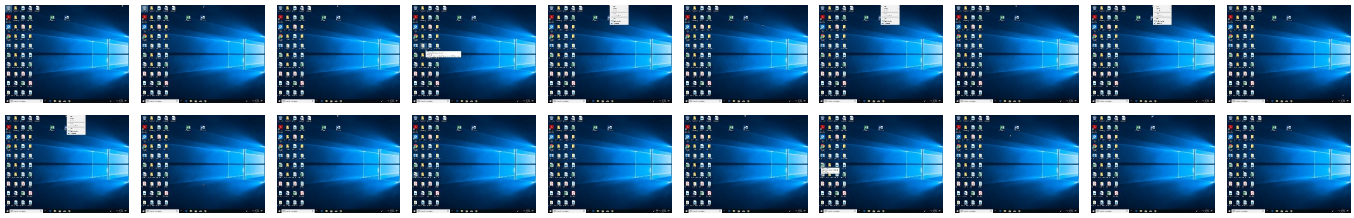
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Products_inquiry.exe	33%	ReversingLabs	Win32.Trojan.Pwsx	
Products_inquiry.exe	36%	Virustotal		Browse
Products_inquiry.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	33%	ReversingLabs	Win32.Trojan.Pwsx	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	36%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
10.2.Products_inquiry.exe.62f0000.17.unpack	100%	Avira	TR/NanoCore.fadte		Download File
10.2.Products_inquiry.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
stevewells.hopto.org	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
stevewells.hopto.org	209.182.100.23	true	true		unknown

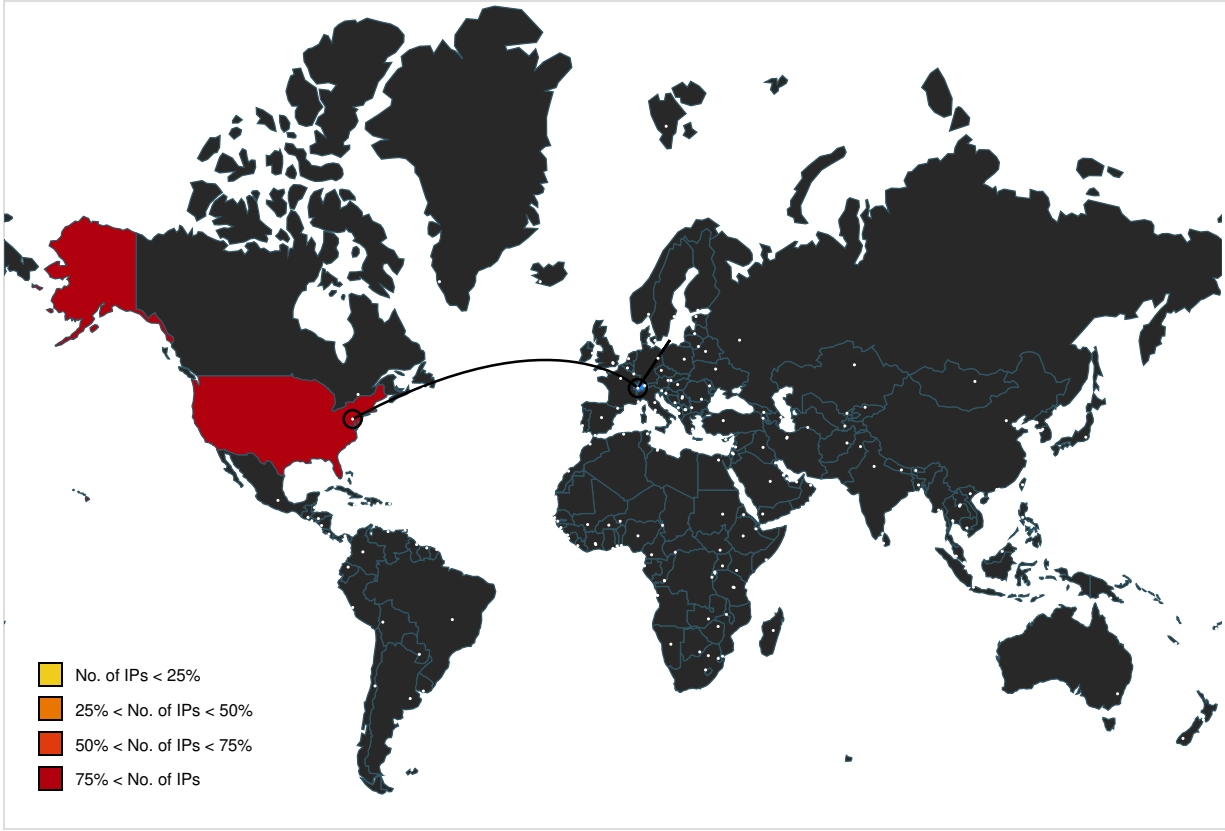
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
stevewells.hopto.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://google.com	Products_inquiry.exe, 0000000A.00000002.525467204.000000000313B000.00000004.00000800.00020000.00000000.sdmp, Products_inquiry.exe, 0000000A.00000002.538870031.00000000043D8000.00000004.00000800.00020000.00000000.sdmp, Products_inquiry.exe, 0000000A.00000002.538870031.00000000041BA000.00000004.00000800.00020000.00000000.sdmp, Products_inquiry.exe, 0000000A.00000002.553746581.0000000007620000.00000004.08000000.00040000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Products_inquiry.exe, 0000000A.00000002.525467204.000000000313B000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
209.182.100.23	stevewells.hopto.org	United States		25693	CLEARPATH-NETWORKSUS	true

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	831164
Start date and time:	2023-03-21 07:21:11 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 22s
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:	14
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	Products_inquiry.exe
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@4/6@3/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed

HCA Information:	• Successful, ratio: 99% • 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, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:23:20	API Interceptor	363x Sleep call for process: Products_inquiry.exe modified
07:23:26	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\Products_inquiry.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	849408
Entropy (8bit):	7.848908391578834
Encrypted:	false
SSDEEP:	24576:JWus7/pDr5Ls+9mWSmwMgHMDviBI3POYQw/:JI0/pDILTIWSmwMgsDKB+r/
MD5:	B4EF6D5785DD94BD5BCE5B980BBFEE62
SHA1:	02C89F672FE728CB334F25D7B0CF90B84584A963

SHA-256:	0FED79A59D3224424DA47A06F87F901E8676A3042F5DC878E095312C3F6C0081
SHA-512:	1A69117AE14553735F1CE88D56017694D9FDD3F9DF5BA906C86F1F2F60715DF90A9844E7E0F60C1E77C38EA93934D24599638C68A275B3409CBA5D507E181374
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 33% • Antivirus: Virustotal, Detection: 36%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....0.d.....0.....>.... ... .@.. .....`..... ..@.....K.... .....@..... ..... ..H.....text...D.... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B..... .....H.....`w.....8-.....0.....8.....E.....8....s.....8....*..(.... ....(....9....&8.....(.....Y.(.....Ys....(.. ..8.....E....'...8".....s....(.... ....(....:....&8.....93...8.....E....!...8.....o.... ....(....:....&8..... ....(....9....&8.....E.\..;....0..>.....(....8.....(.... .....:....& ....8....8.....E..... 8....*..*....(....*.:.....o....*.:.....(....*.&~.....*...~..

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

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

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

Process:	C:\Users\user\Desktop\Products_inquiry.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

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

Process:	C:\Users\user\Desktop\Products_inquiry.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	3:XrURGizD7cnRNGbgCFKRNX/pBK0jCV83ne+VdWPiKgmR7kkmefoeLBizbCuVkqYM:X4LDAnybgCFcps0OafmCYDlizZr/i/Oh
MD5:	9E7D0351E4DF94A9B0BADCEB6A9DB963
SHA1:	76C6A69B1C31CEA2014D1FD1E222A3DD1E433005

SHA-256:	AAFC7B40C5FE680A2BB549C3B90AABAAC63163F74FFFC0B00277C6BBFF88B757
SHA-512:	93CCF7E046A3C403ECF8BC4F1A8850BA0180FE18926C98B297C5214EB77BC212C8FBCC58412D0307840CF2715B63BE68BACDA95AA98E82835C5C53F17EF3851
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+.....*....~f.G0^..;....W2.=...K.~.L..&f...p.....:7rH}..../H.....L...?...A.K...J.=8x!....+ .2e'..E?.G.....[.&

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

Process:	C:\Users\user\Desktop\Products_inquiry.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:7+t:6t
MD5:	DB4458B3CC6AF634B6B96C428F0706E5
SHA1:	9B9220190B1BA5F922DDAD77275982EECD4DAA98
SHA-256:	F06ACA77E11B56ECEB2207DAB444F34995C70D21B07AF7A145643F3104E8C94D
SHA-512:	8C2043DC0FBC8684F172BB3943989DCA88426083A38C2F51FBB989DAADE37011D5AA2255038BA31D1045A1F736DC3C41478B8F45E3750B8C8587CF6E693C7BA
Malicious:	**true**
Reputation:	low
Preview:	+.n..*.H

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

Process:	C:\Users\user\Desktop\Products_inquiry.exe
File Type:	data
Category:	modified
Size (bytes):	327768
Entropy (8bit):	**7.999367066417797**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3PlZmqze1d1wI8lkWmtjJ/3Exi:LkjbU7LjGxi
MD5:	2E52F446105FBF828E63CF808B721F9C
SHA1:	5330E54F238F46DC04C1AC62B051DB4FCD7416FB
SHA-256:	2F7479AA2661BD259747BC89106031C11B3A3F79F12190E7F19F5DF65B7C15C8
SHA-512:	C08BA0E3315E2314ECBEF38722DF834C2CB8412446A9A310F41A8F83B4AC5984FCC1B26A1D8B0D58A730FDBDD885714854BDFD04DCDF7F582FC125F552D5C3CA
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.848908391578834
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:	Products_inquiry.exe
File size:	849408
MD5:	b4ef6d5785dd94bd5bce5b980bbfee62
SHA1:	02c89f672fe728cb334f25d7b0cf90b84584a963
SHA256:	0fed79a59d3224424da47a06f87f901e8676a3042f5dc878e095312c3f6c0081
SHA512:	1a69117ae14553735f1ce88d56017694d9fdd3f9df5ba906c86f1f2f60715df90a9844e7e0f60c1e77c38ea93934d24599638c68a275b3409cba5d507e181374

SSDEEP:	24576:JWus7/pDr5Ls+9mWSmwMgHMDviBI3POYQw/:Jl0/pDlLTIWSmwMgsDKB+r/
TLSH:	5E05025B37999912C3992939C2D7812807B5A8432733DA493CC613962E0F7E95D8EFCF
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....0.d..............0.............>.... ... .@.. ....`............@................................

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d0a3e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x641930BF [Tue Mar 21 04:21:19 2023 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]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd09f0	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd2000	0x5d0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd4000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xd09ab	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

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xcea44	0xcec00	False	0.9182072815900847	data	7.855251753223261	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x5d0	0x600	False	0.4270833333333333	data	4.139332907247123	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	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	0xd20a0	0x344	data		
RT_MANIFEST	0xd23e4	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Imports

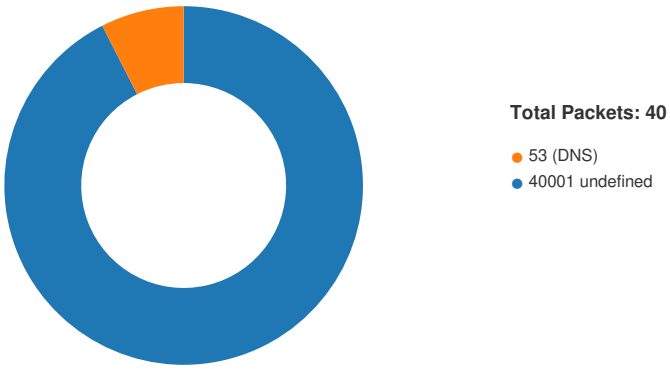
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.3209.182.100.2349697400012816766 03/21/23-07:23:30.034206	TCP	2816766	ETPRO TROJAN NanoCore RAT CnC 7	49697	40001	192.168.2.3	209.182.100.23
192.168.2.3209.182.100.2349697400012025019 03/21/23-07:23:28.411292	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49697	40001	192.168.2.3	209.182.100.23

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:23:27.767009020 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:27.905769110 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:27.905999899 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:28.411292076 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:28.565323114 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:28.565447092 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:28.756023884 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:28.756124020 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:28.895087004 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:28.935720921 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:28.980143070 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.173826933 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.173976898 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.183818102 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.183873892 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.183954000 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.183986902 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.183986902 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.184039116 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.184063911 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.184118032 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.322676897 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.322788000 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.322858095 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.322921991 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.322947979 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.322971106 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.323019028 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.323021889 CET	49697	40001	192.168.2.3	209.182.100.23

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:23:29.323064089 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.323088884 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.323110104 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.323173046 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.461725950 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.461771965 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.461811066 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.461849928 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.461880922 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.461889029 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.461922884 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.461930037 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.461971045 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462011099 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462027073 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.462050915 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462061882 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.462090015 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462130070 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462167978 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462187052 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.462207079 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462224007 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.462244034 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462285042 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462323904 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.462342024 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.462378025 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.601161003 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601224899 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601274014 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601310015 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.601320982 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601370096 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601388931 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.601419926 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601468086 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601514101 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601526976 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.601560116 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601569891 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.601605892 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601654053 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601694107 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.601701021 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601749897 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601798058 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601810932 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.601846933 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601855993 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.601895094 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601942062 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601989031 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.601995945 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.602034092 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602045059 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.602082014 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602128983 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602175951 CET	40001	49697	209.182.100.23	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:23:29.602185965 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.602221966 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602232933 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.602268934 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602315903 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602363110 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602384090 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.602408886 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602420092 CET	49697	40001	192.168.2.3	209.182.100.23
Mar 21, 2023 07:23:29.602458954 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602505922 CET	40001	49697	209.182.100.23	192.168.2.3
Mar 21, 2023 07:23:29.602562904 CET	40001	49697	209.182.100.23	192.168.2.3

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 21, 2023 07:23:27.731719017 CET	62704	53	192.168.2.3	8.8.8.8
Mar 21, 2023 07:23:27.753777981 CET	53	62704	8.8.8.8	192.168.2.3
Mar 21, 2023 07:23:36.737576008 CET	49977	53	192.168.2.3	8.8.8.8
Mar 21, 2023 07:23:36.757720947 CET	53	49977	8.8.8.8	192.168.2.3
Mar 21, 2023 07:23:41.007380009 CET	57840	53	192.168.2.3	8.8.8.8
Mar 21, 2023 07:23:41.029992104 CET	53	57840	8.8.8.8	192.168.2.3

DNS Queries

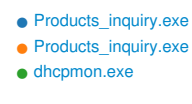
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 21, 2023 07:23:27.731719017 CET	192.168.2.3	8.8.8.8	0xf8cb	Standard query (0)	stevewells .hopto.org	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:23:36.737576008 CET	192.168.2.3	8.8.8.8	0x1606	Standard query (0)	stevewells .hopto.org	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:23:41.007380009 CET	192.168.2.3	8.8.8.8	0x456d	Standard query (0)	stevewells .hopto.org	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 21, 2023 07:23:27.753777981 CET	8.8.8.8	192.168.2.3	0xf8cb	No error (0)	stevewells .hopto.org		209.182.100.23	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:23:36.757720947 CET	8.8.8.8	192.168.2.3	0x1606	No error (0)	stevewells .hopto.org		209.182.100.23	A (IP address)	IN (0x0001)	false
Mar 21, 2023 07:23:41.029992104 CET	8.8.8.8	192.168.2.3	0x456d	No error (0)	stevewells .hopto.org		209.182.100.23	A (IP address)	IN (0x0001)	false

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: Products_inquiry.exe PID: **5568**, Parent PID: **3452**

General

Target ID:	0
Start time:	07:22:03
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\Products_inquiry.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Products_inquiry.exe
Imagebase:	0x100000
File size:	849408 bytes
MD5 hash:	B4EF6D5785DD94BD5BCE5B980BBFEE62
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Products_inquiry.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72CAC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Products_inquiry.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	72CAC907	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Analysis Process: Products_inquiry.exe PID: **4124**, Parent PID: **5568**

General

Target ID:	10
Start time:	07:23:20
Start date:	21/03/2023
Path:	C:\Users\user\Desktop\Products_inquiry.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Products_inquiry.exe
Imagebase:	0xba0000
File size:	849408 bytes
MD5 hash:	B4EF6D5785DD94BD5BCE5B980BBFEE62
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: 0000000A.00000002.538870031.00000000040F1000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.550430211.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.550430211.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.550430211.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.550430211.0000000006800000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.538870031.0000000004141000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.538870031.0000000004141000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.553366614.00000000075E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.553366614.00000000075E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.553366614.00000000075E0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.553366614.00000000075E0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.525467204.000000000313B000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.525467204.000000000313B000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.552557346.0000000007460000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.552557346.0000000007460000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.552557346.0000000007460000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.552557346.0000000007460000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.538870031.00000000043D8000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.538870031.00000000043D8000.00000004.00000800.00020000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.553746581.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.553746581.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.553746581.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.553746581.0000000007620000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.556271335.00000000077A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.556271335.00000000077A0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.556271335.00000000077A0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.556271335.00000000077A0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.549608665.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.549608665.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.549608665.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.549608665.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.549608665.00000000062F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.553441072.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.553441072.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.553441072.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.553441072.00000000075F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.556689984.00000000077B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.556689984.00000000077B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.556689984.00000000077B0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.556689984.00000000077B0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.549280974.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.549280974.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)
- Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.549280974.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
- Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.549280974.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.557503745.00000000077F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems)

	• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.557503745.00000000077F0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.557503745.00000000077F0000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.557503745.00000000077F0000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.515027451.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.515027451.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.515027451.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.515027451.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.553567509.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.553567509.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.553567509.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.553567509.0000000007600000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000A.00000002.538870031.00000000041BA000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000A.00000002.538870031.00000000041BA000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.538870031.00000000041BA000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.553890216.0000000007630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.553890216.0000000007630000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.553890216.0000000007630000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.553890216.0000000007630000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.554138869.0000000007640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.554138869.0000000007640000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.554138869.0000000007640000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.554138869.0000000007640000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000A.00000002.553643696.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000A.00000002.553643696.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth (Nextron Systems) • Rule: MALWARE_Win_NanoCore, Description: Detects NanoCore, Source: 0000000A.00000002.553643696.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000002.553643696.0000000007610000.00000004.08000000.00040000.00000000.sdmp, Author: unknown • Rule: Windows_Trojan_Nanocore_d8c4e3c5, Description: unknown, Source: 0000000A.00000003.430716951.00000000070E1000.00000004.00000020.00020000.00000000.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	7299CF06	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	7299CF06	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	717EBEFF	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	717E1E60	CreateFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	717EDD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	717EBEFF	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	717EBEFF	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	1	717E1E60	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	717E1E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Products_inquiry.exe:Zone.Identifier	success or wait	1	56A88F6	DeleteFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	2b fd 6e fd 17 2a fd 48	+n*H	success or wait	1	717E1B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 30 19 64 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 30 00 00 fd 0c 00 00 08 00 00 00 00 00 00 3e 0a 0d 00 00 20 00 00 00 20 0d 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0d 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 0f 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PEL0d0> @ `@	success or wait	4	717EDD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	717EDD66	CopyFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 3b fd fd 04 20 53 fd 12 1c fd 7d 46 46 fd 32 fd fd fd 68 fd 4d 2b fd 39 fd fd 4c fd 23 fd 58 fd fd 2b fd fd fd 01 fd fd 2a fd fd 1e fd 7e 66 1e 47 30 5e e9 56 3b fd 2e fd fd 57 32 fd 3d 10 fd fd 4b fd 7e fd 4c 1f 15 26 66 fd fd 2e 70 fd 04 1b fd fd fd 0f fd fd fd 0b 10 3a 37 72 48 7d fd fd fd 0d 2f 48 16 fd fd 06 17 fd 4c fd fd 04 3f fd fd 04 41 08 4b 07 fd fd 4a 17 3d 38 78 21 19 fd fd fd 2b fd 32 65 27 fd 1f 45 3f fd 47 11 fd fd fd 01 fd 5b 00 26	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i S}FF2hM+L#X+*~fG0^;. W2=K~L&f.p:7rH}/HL? AKJ=8x!+2e'E?G[&	success or wait	1	717E1B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327768	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	717E1B4F	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	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7295D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7295D72F	unknown
C:\Users\user\Desktop\Products_inquiry.exe	unknown	4096	success or wait	1	7295D72F	unknown
C:\Users\user\Desktop\Products_inquiry.exe	unknown	512	success or wait	1	7295D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	717E646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: **2008**, Parent PID: **3452**

General

Target ID:	13
Start time:	07:23:35
Start date:	21/03/2023
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0xa0000
File size:	849408 bytes
MD5 hash:	B4EF6D5785DD94BD5BCE5B980BBFEE62
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 33%, ReversingLabs • Detection: 36%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7299CF06	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	7299CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	72975705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7297CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	728D03DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	728D03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	728D03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	72975705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	717E1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	717E1B4F	ReadFile

Disassembly

No disassembly