ID: 483496
Sample Name: P0 (2021)-2790
new order.exe
Cookbook: default.jbs
Time: 06:12:21
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

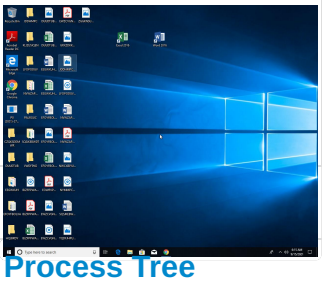
Windows Analysis Report P0 (2021)-2790 new order.exe

Overview

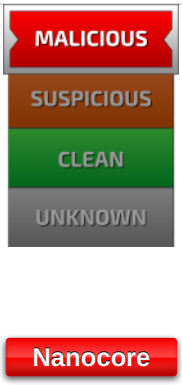
General Information

Sample Name:	P0 (2021)-2790 new order.exe
Analysis ID:	483496
MD5:	394ff651c9fa2bfc..
SHA1:	e9ae9e9c2985aa..
SHA256:	25cc795662dc5f4..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

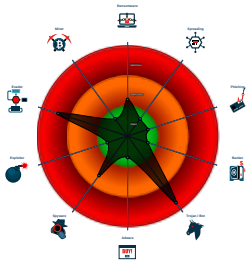


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Detected Nanocore Rat
- Multi AV Scanner detection for doma…
- Yara detected Nanocore RAT
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w10x64**
- P0 (2021)-2790 new order.exe (PID: 6380 cmdline: 'C:\Users\user\Desktop\P0 (2021)-2790 new order.exe' MD5: 394FF651C9FA2BFCA16C32FB117514E1)
  - conhost.exe (PID: 6388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 6440 cmdline: 'C:\Users\user\Desktop\P0 (2021)-2790 new order.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 6652 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7C69.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6676 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6724 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp8052.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6732 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 6824 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 6832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6840 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 6848 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 7028 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 7036 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6e073bd7-7c11-48c2-8a90-355dddea",
  "Group": "Default",
  "Domain1": "185.140.53.8",
  "Domain2": "",
  "Port": 8907,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Enable",
  "BypassUAC": "Enable",
  "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": "",
  "BackupDNSServer": "185.140.53.8",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.479823366.000000000402000.00000040.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000002.00000002.479823366.000000000402000.00000040.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000002.00000002.479823366.000000000402000.00000040.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000002.00000002.484597915.00000000040C9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000002.00000002.485007729.0000000005A20000.00000004.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost

Click to see the 14 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.MSBuild.exe.5cc0000.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
2.2.MSBuild.exe.5cc0000.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
2.2.MSBuild.exe.5cc0000.6.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
2.2.MSBuild.exe.40d7a70.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
2.2.MSBuild.exe.40d7a70.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
Click to see the 29 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Yara detected Nanocore RAT

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

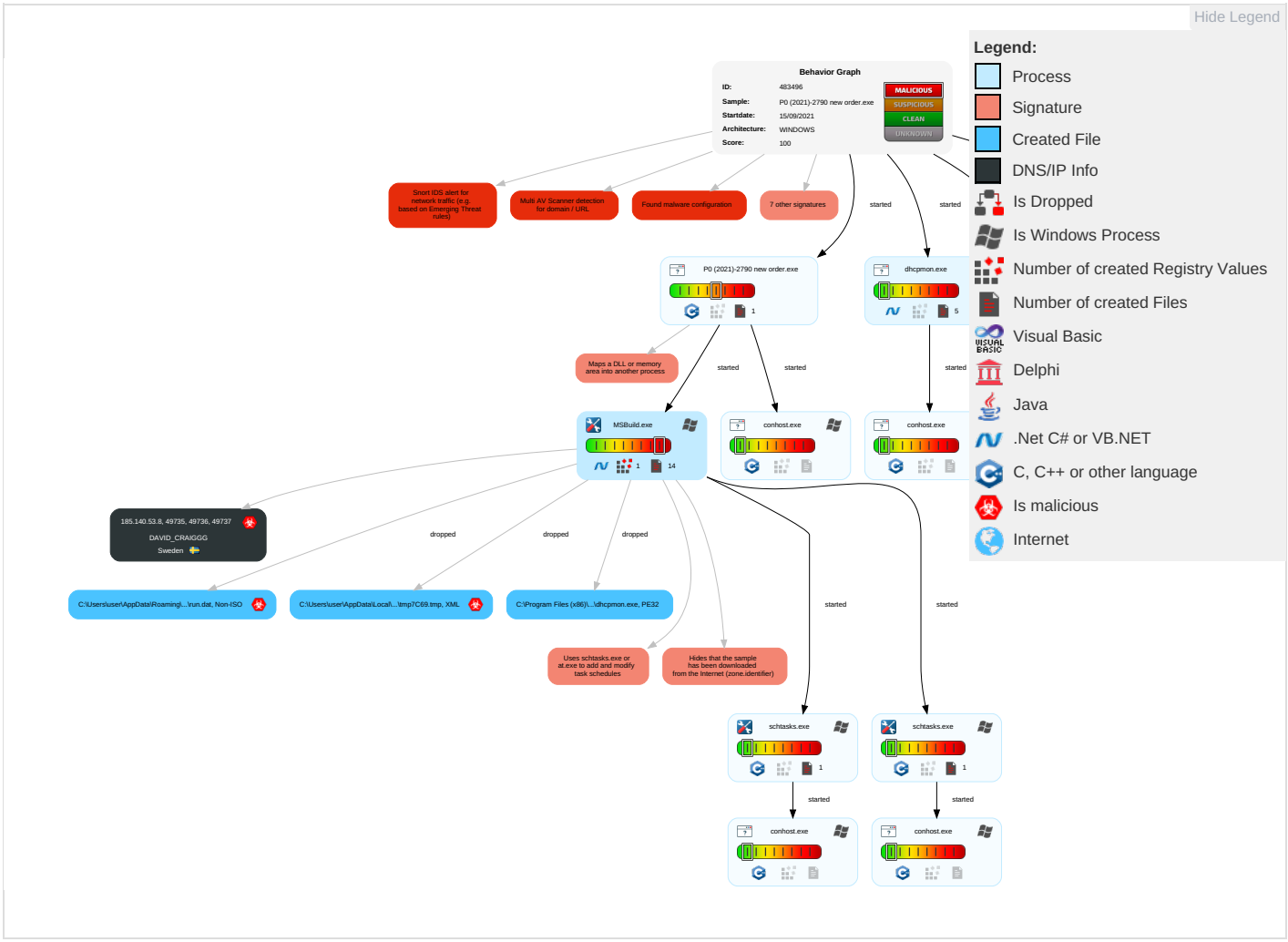
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts	Scheduled Task/Job 1	Windows Service 3	Access Token Manipulation 1	Masquerading 2	Input Capture 2 1	System Time Discovery 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eave Insec Netw Com
Default Accounts	Service Execution 2	Scheduled Task/Job 1	Windows Service 3	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Explo Redi Calls
Domain Accounts	At (Linux)	Application Shimming 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Explo Track Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Access Token Manipulation 1	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Ingress Tool Transfer 1	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Application Shimming 1	Process Injection 1 1 2	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Mani Devic Com
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 3 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamr Denia Servi
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insec Protc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 1 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

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

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	1%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.MSBuild.exe.5cc0000.6.unpack	100%	Avira	TR/NanoCore.fadte		Download File
2.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
185.140.53.8	11%	Virustotal		Browse
185.140.53.8	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
185.140.53.8	true	• 11%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.8	unknown	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483496
Start date:	15.09.2021
Start time:	06:12:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 17s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	P0 (2021)-2790 new order.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	35
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@16/11@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 68% (good quality ratio 61.8%) • Quality average: 80.4% • Quality standard deviation: 31.6%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
06:13:22	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
06:13:24	API Interceptor	997x Sleep call for process: MSBuild.exe modified
06:13:25	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe" s>$(Arg0)
06:13:25	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.8	I8Bg3M4Obd.exe	Get hash	malicious	Browse	
	MANILA LGU VACCINATION.exe	Get hash	malicious	Browse	
	Memorandum.pdf.exe	Get hash	malicious	Browse	
	Scan copy ref PDF.exe	Get hash	malicious	Browse	
	CV CREDENTIALS.exe	Get hash	malicious	Browse	
	WeASwOPOdNuVKbq.exe	Get hash	malicious	Browse	
	Purchase order.exe	Get hash	malicious	Browse	
	SWIFT GIHTLDOM00000003078.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	HEIpSUdxRf.exe	Get hash	malicious	Browse	• 185.140.53.11
	SPT DRINGENDE BESTELLUNG _876453,pdf.exe	Get hash	malicious	Browse	• 91.193.75.133
	MAERSK ARRIVAL NOTICE.exe	Get hash	malicious	Browse	• 185.140.53.142
	MHHHG_9847654673T3RDNVAASGU.NET.exe	Get hash	malicious	Browse	• 185.140.53.9
	ordine 338390208,pdf.exe	Get hash	malicious	Browse	• 185.140.53.11
	Final Order.exe	Get hash	malicious	Browse	• 185.140.53.133
	SecuriteInfo.com.BackDoor.SpyBotNET.25.7070.exe	Get hash	malicious	Browse	• 185.140.53.9
	yu8jcWMYUw.exe	Get hash	malicious	Browse	• 185.140.53.76
	UK COVID UPDATES AND ENTITLEMENT.exe	Get hash	malicious	Browse	• 91.193.75.202
	TWM#U007e-04987474848GRRT.exe	Get hash	malicious	Browse	• 185.140.53.9
	BankSlip.exe	Get hash	malicious	Browse	• 185.140.53.226
	Bank-Slip.exe	Get hash	malicious	Browse	• 185.140.53.226
	HSBC -- Wire Transfer copy.exe	Get hash	malicious	Browse	• 91.193.75.173
	lol.exe	Get hash	malicious	Browse	• 185.140.53.216
	PO N. ordine 338390208B,pdf.exe	Get hash	malicious	Browse	• 185.140.53.11
	Confirma#U00e7#U00e3o do pedido _ Urgente,pdf.exe	Get hash	malicious	Browse	• 91.193.75.133
	Acil RFQ_AP65425652_032421.exe	Get hash	malicious	Browse	• 185.140.53.11
	Auftragsbest#U00e4tigung _ Dringend,pdf.exe	Get hash	malicious	Browse	• 91.193.75.133
	qkWaxZQ3dW.exe	Get hash	malicious	Browse	• 91.193.75.173
	HPEE IMAGES-SPECIFICATION ORDER - Copy.xlsm	Get hash	malicious	Browse	• 91.193.75.173

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	TNT AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	
	BankSlip.exe	Get hash	malicious	Browse	
	PAYMENT ERROR.exe	Get hash	malicious	Browse	
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	
	DHL AWB TRACKING DETAILS.exe	Get hash	malicious	Browse	
	PcgYFOwcNQ.exe	Get hash	malicious	Browse	
	Invoice Fanpage Karma.bat.exe	Get hash	malicious	Browse	
	zslaUKmBfr.exe	Get hash	malicious	Browse	
	scanbankdoc210999796432225.bat.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.Variant.Zusy.394472.4088.exe	Get hash	malicious	Browse	
	SecuriteInfo.com.W32.AIDetect.malware1.17748.exe	Get hash	malicious	Browse	
	fnnEkbo4cW.exe	Get hash	malicious	Browse	
	kAGA3XtSEaOxfvA.exe	Get hash	malicious	Browse	
	PO 18-3081.exe	Get hash	malicious	Browse	
	Order417.exe	Get hash	malicious	Browse	
	PCT0002982765627827BC.exe	Get hash	malicious	Browse	
	NO19800800.exe	Get hash	malicious	Browse	
	NAO09009009.exe	Get hash	malicious	Browse	
	SYT09009.exe	Get hash	malicious	Browse	
	RFQEMFA.Elektrik.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	69632
Entropy (8bit):	5.20894581699571
Encrypted:	false
SSDEEP:	768:NElGiBcBuiyFjUwF0wdP9/rJMDnRFRJfStGpwV3e3qtAcy:ilGBu7jjP9/tMDn9Jt+VO3GO
MD5:	88BBB7610152B48C2B3879473B17857E
SHA1:	0F6CF8DD66AA58CE31DA4E8AC0631600EF055636
SHA-256:	2C7ACC16D19D076D67E9F1F37984935899B79536C9AC6EEC8850C44D20F87616
SHA-512:	5BACDF6C190A76C2C6A9A3519936E08E898AC8A2B1384D60429DF850BE778860435BF9E5EB316517D2345A5AAE201F369863F7A242134253978BCB5B2179CA58
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 1%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: TNT AWB TRACKING DETAILS.exe, Detection: malicious, Browse • Filename: BankSlip.exe, Detection: malicious, Browse • Filename: PAYMENT ERROR.exe, Detection: malicious, Browse • Filename: DHL AWB TRACKING DETAILS.exe, Detection: malicious, Browse • Filename: DHL AWB TRACKING DETAILS.exe, Detection: malicious, Browse • Filename: PcgYFOwcNQ.exe, Detection: malicious, Browse • Filename: Invoice Fanpage Karma.bat.exe, Detection: malicious, Browse • Filename: zslaUKmBfr.exe, Detection: malicious, Browse • Filename: scanbankdoc210999796432225.bat.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.Variant.Zusy.394472.4088.exe, Detection: malicious, Browse • Filename: SecuriteInfo.com.W32.AIDetect.malware1.17748.exe, Detection: malicious, Browse • Filename: fnnEkbo4cW.exe, Detection: malicious, Browse • Filename: kAGA3XtSEaOxfvA.exe, Detection: malicious, Browse • Filename: PO 18-3081.exe, Detection: malicious, Browse • Filename: Order417.exe, Detection: malicious, Browse • Filename: PCT0002982765627827BC.exe, Detection: malicious, Browse • Filename: NO19800800.exe, Detection: malicious, Browse • Filename: NAO09009009.exe, Detection: malicious, Browse • Filename: SYT09009.exe, Detection: malicious, Browse • Filename: RFQEMFA.Elektrik.exe, Detection: malicious, Browse

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....{Z.....@..... .....@.. .....@.....99.. ..@.....S.....`/..... ..... ..H.....text..... ..... ..`.rsrc...`/.....0.....@..@.reloc..... . .....@..B.....

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\MSBuild.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	325
Entropy (8bit):	5.334380084018418
Encrypted:	false
SSDEEP:	6:Q3LadLCR22lAQykdL1tZbLsbFLIP12MUAvvro6ysGMFLIP12MUAvvrs:Q3LaJU20NaL1tZbgbe4MqJsGMe4M6
MD5:	65CE98936A67552310EFE2F0FF5BDF88
SHA1:	8133653A6B9A169C7496ADE315CED322CFC3613A
SHA-256:	682F7C55B1B6E189D17755F74959CD08762F91373203B3B982ACFFCADE2E871A
SHA-512:	2D00AC024267EC384720A400F6D0B4F7EDDF49FAF8AB3C9E6CBFBBAE90ECADACA9022B33E3E8EC92E4F57C7FC830299C8643235EB4AA7D8A6AFE9DD1775F57C3
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	441
Entropy (8bit):	5.388715099859351
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U2+gYhD5itZbgbe4MqJsGMe4M6:MLF20NaL32+g2OH4xvn4j
MD5:	88F0104DB9A3F9BC4F0FC3805F571B0D
SHA1:	CDD4F34385792F0CCE0A844F4ABB447C25AB4E73
SHA-256:	F6C11D3D078ED73F2640DA510E68DEEAA5F14F79CAE2E23A254B4E37C7D0230F
SHA-512:	04B977F63CAB8DE20EA7EFA9D4299C2E625D92FA6D54CA03EECD9F322E978326B353824F23BEC0E712083BDE0DBC5CC4EE90922137106B096050CA46A166DFE
Malicious:	false
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Xml\527c933194f3a99a816d83c619a3e1d3\System.Xml.ni.dll",0..2,"Microsoft.Build.Engine, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build.Framework, Version=2.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Temp\tmp7C69.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.136963558289723
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mnc2xtn:cbk4oL600QydbQxIYODOLedq3ZLj
MD5:	AE766004C0D8792953BAFFFE8F6A2E3B
SHA1:	14B12F27543A401E2FE0AF8052E116CAB0032426
SHA-256:	1ABDD9B6A6B84E4BA1AF1282DC84CE276C59BA253F4C4AF05FEA498A4FD99540
SHA-512:	E530DA4A5D4336FC37838D0E93B5EB3804B9C489C71F6954A47FC81A4C655BB72EC493E109CF96E6E3617D7623AC80697AD3BBD5FFC6281BAFC8B34DCA5E657
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp8052.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators

C:\Users\user\AppData\Local\Temp\tmp8052.tmp	
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	2320
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwh:flC0IlC0IlC0IlC0IlC0IlC0IlC0IlCr
MD5:	0FBED11864C03FDED0E70014DCF84578
SHA1:	453723D938A03252F705B0A104986FE4C5CA7056
SHA-256:	70F5E49EE3091777827ED661B63842061220C899A708860986E9AA1BD87C5004
SHA-512:	DB53E3F1D18171F1D86C1B9BBF6BBD07153FC3E561834A35834BC0CA1E034FEDCD83AAAE7EDF9262C4E175C3D2287B647F55282E49627EAAF587F4371420466
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7.." .hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0.:e[7w{1.!.4.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	Non-ISO extended-ASCII text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:TIF8:i8
MD5:	EFCA6CC477D60399732B834743979140
SHA1:	FD4A75B0CFD84A9FE784E6C9E2ACD1A3CF235F52
SHA-256:	3AE30778C66035457B34DF8B5A96CAE81968B115B46EC5CBFCE442235E0268DD
SHA-512:	408636EFBD4BAA30CD78AD0F450ADD2D8937D6F0FDD49DA8D7F105279E148017F472371E954F3A0F9CCA59DB18EBBB82F1758F05E6312EFEAECA51212DEF696
Malicious:	**true**
Preview:	M+..Jx.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.85263908467479
Encrypted:	false
SSDEEP:	3:oMty8WbSI1u:oMLWuI1u
MD5:	A35128E4E28B27328F70E4E8FF482443
SHA1:	B89066B2F8DB34299AABFD7ABEE402D5444DD079
SHA-256:	88AEA00733DC4B570A29D56A423CC5BF163E5ACE7AF349972EB0BBA8D9AD06E1
SHA-512:	F098E844B5373B34642B49B6E0F2E15CFDAA1A8B6CABC2196CEC0F3765289E5B1FD4AB588DD65F97C8E51FA9A81077621E9A06946859F296904C646906A70F33

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	306
Entropy (8bit):	4.969261552825097
Encrypted:	false
SSDEEP:	6:zx3M1tlAX8bSWR30qysGMQbSVRRZBXVRbJ0fFdCsq2UTiMdH8stCal+n:zK1XnV30ZsGMIG9BFRbQdCT2UftCM+
MD5:	F227448515085A647910907084E6728E
SHA1:	5FA1A8E28B084DA25A1BBC51A2D75810CEF57E2C
SHA-256:	662BA47D628FE8EBE95DD47B4482110A10B49AED09387BC0E028BB66E68E20BD
SHA-512:	6F6E5DFFF7B17C304FB19B0BA5466AF84EF98A5C2EFA573AF72CFD3ED6964E9FD7F8E4B79FCFFBEF87CE545418C69D4984F4DD60BBF457D0A3640950F8FC5AF0
Malicious:	false
Preview:	Microsoft (R) Build Engine Version 2.0.50727.8922..[Microsoft .NET Framework, Version 2.0.50727.8922]..Copyright (C) Microsoft Corporation 2005. All rights reserved.....MSBUILD : error MSB1003: Specify a project or solution file. The current working directory does not contain a project or solution file...

Static File Info

General

File type:	PE32 executable (console) Intel 80386, for MS Windows
Entropy (8bit):	7.650091855564988
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	P0 (2021)-2790 new order.exe
File size:	349184
MD5:	394ff651c9fa2bfca16c32fb117514e1
SHA1:	e9ae9e9c2985aaa1c96c7186f9147eebddb7b203
SHA256:	25cc795662dc5f48d3e7dc1fcab5add2deed04887f7cfef18d1d4a3d7abf5ee7
SHA512:	d2d78bbf59d3023e219f24f7291b68a7dae9fe414812debfcc669572c392e00b232b80e94ba90fad797ae98d7ac402301cb9f46143b0e618207faefd5a1457e1
SSDEEP:	6144:tVQdPFh9YpnPSh80181yMJvS9Q4swk/qRdEt92V:c9T9W6h87P41kkdEzW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u.....Rich.....PE..L..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x402abf
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

General

DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61411185 [Tue Sep 14 21:17:57 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	337cc3ba01595b56bed66bb7d8f07a5a

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x17f49	0x18000	False	0.516937255859	data	6.60931791398	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x19000	0x6002	0x6200	False	0.370894451531	data	4.53614585813	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x20000	0x31c4	0x1400	False	0.320703125	data	3.52089438859	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x24000	0x345e8	0x34600	False	0.966983330847	data	7.99013268015	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x59000	0x13c8	0x1400	False	0.81640625	data	6.61096020071	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-06:13:25.405871	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49735	8907	192.168.2.3	185.140.53.8
09/15/21-06:13:31.501018	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49736	8907	192.168.2.3	185.140.53.8
09/15/21-06:13:38.187895	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49737	8907	192.168.2.3	185.140.53.8
09/15/21-06:13:44.206046	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	8907	192.168.2.3	185.140.53.8
09/15/21-06:13:50.209237	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	8907	192.168.2.3	185.140.53.8
09/15/21-06:13:56.944143	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	8907	192.168.2.3	185.140.53.8

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/15/21-06:14:01.984974	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:06.785682	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:12.820795	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49774	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:18.902806	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49775	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:23.515493	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49779	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:29.704539	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49786	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:35.710881	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49787	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:41.780948	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49788	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:48.141045	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49789	8907	192.168.2.3	185.140.53.8
09/15/21-06:14:54.128708	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49790	8907	192.168.2.3	185.140.53.8
09/15/21-06:15:00.100074	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49795	8907	192.168.2.3	185.140.53.8
09/15/21-06:15:06.102195	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49796	8907	192.168.2.3	185.140.53.8
09/15/21-06:15:12.099261	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49797	8907	192.168.2.3	185.140.53.8
09/15/21-06:15:18.180591	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49798	8907	192.168.2.3	185.140.53.8
09/15/21-06:15:24.133637	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49799	8907	192.168.2.3	185.140.53.8

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: P0 (2021)-2790 new order.exe PID: 6380 Parent PID: 2308

General

Start time:	06:13:17
Start date:	15/09/2021

Path:	C:\Users\user\Desktop\P0 (2021)-2790 new order.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\P0 (2021)-2790 new order.exe'
Imagebase:	0xa30000
File size:	349184 bytes
MD5 hash:	394FF651C9FA2BFCA16C32FB117514E1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.223144000.0000000002720000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.223144000.0000000002720000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.223144000.0000000002720000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.223144000.0000000002720000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6388 Parent PID: 6380

General

Start time:	06:13:18
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: MSBuild.exe PID: 6440 Parent PID: 6380

General

Start time:	06:13:18
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\P0 (2021)-2790 new order.exe'
Imagebase:	0x9e0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
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: 00000002.00000002.479823366.0000000000402000.00000040.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.479823366.0000000000402000.00000040.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000002.00000002.479823366.0000000000402000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.484597915.00000000040C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.485007729.0000000005A20000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.485007729.0000000005A20000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000002.00000002.485086472.0000000005CC0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000002.00000002.485086472.0000000005CC0000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000002.00000002.485086472.0000000005CC0000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 6652 Parent PID: 6440

General

Start time:	06:13:22
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp7C69.tmp'
Imagebase:	0x940000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6676 Parent PID: 6652

General

Start time:	06:13:22
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6724 Parent PID: 6440

General

Start time:	06:13:23
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp8052.tmp'
Imagebase:	0x940000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6732 Parent PID: 6724

General

Start time:	06:13:23
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: MSBuild.exe PID: 6824 Parent PID: 528

General

Start time:	06:13:25
Start date:	15/09/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0
Imagebase:	0xfb0000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6832 Parent PID: 6824

General

Start time:	06:13:25
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: dhcpmon.exe PID: 6840 Parent PID: 528

General

Start time:	06:13:25
Start date:	15/09/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0x40000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 1%, Virustotal, Browse • Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6848 Parent PID: 6840

General

Start time:	06:13:26
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: dhcpmon.exe PID: 7028 Parent PID: 3388

General

Start time:	06:13:31
Start date:	15/09/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xf60000
File size:	69632 bytes
MD5 hash:	88BBB7610152B48C2B3879473B17857E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 7036 Parent PID: 7028

General

Start time:	06:13:31
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis