ID: 458451
Sample Name: Orderlist.exe
Cookbook: default.jbs
Time: 11:33:46
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

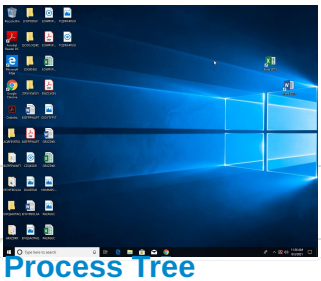
Windows Analysis Report Orderlist.exe

Overview

General Information

Sample Name:	Orderlist.exe
Analysis ID:	458451
MD5:	57201aec028c2b..
SHA1:	150471c9ac6f432..
SHA256:	580eb6d5dffc61f…
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

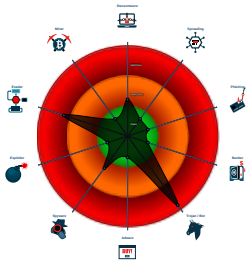
Nanocore

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- Orderlist.exe (PID: 5836 cmdline: 'C:\Users\user\Desktop\Orderlist.exe' MD5: 57201AEC028C2BD9A91E79ED81AEB868)
  - MSBuild.exe (PID: 5796 cmdline: 'C:\Users\user\Desktop\Orderlist.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 1628 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmpD5BB.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1324 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 4204 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
    - conhost.exe (PID: 1188 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "8a1be7ed-1b25-4346-8844-80b424a6",
  "Group": "Default",
  "Domain1": "sobe123.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 5656,
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5024,
  "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",
  "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
00000001.00000002.236917800.000000000385 0000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.236917800.000000000385 0000.00000040.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
00000001.00000002.236917800.000000000385 0000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000002.236917800.000000000385 0000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q

Source	Rule	Description	Author	Strings
Process Memory Space: Orderlist.exe PID: 5836	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xde3:$x1: NanoCore.ClientPluginHost • 0xe20:$x2: IClientNetworkHost • 0x4911:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xf997:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Orderlist.exe.3850000.2.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1.2.Orderlist.exe.3850000.2.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
1.2.Orderlist.exe.3850000.2.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.Orderlist.exe.3850000.2.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
1.2.Orderlist.exe.3850000.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 3 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 submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Uses dynamic DNS services

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

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:

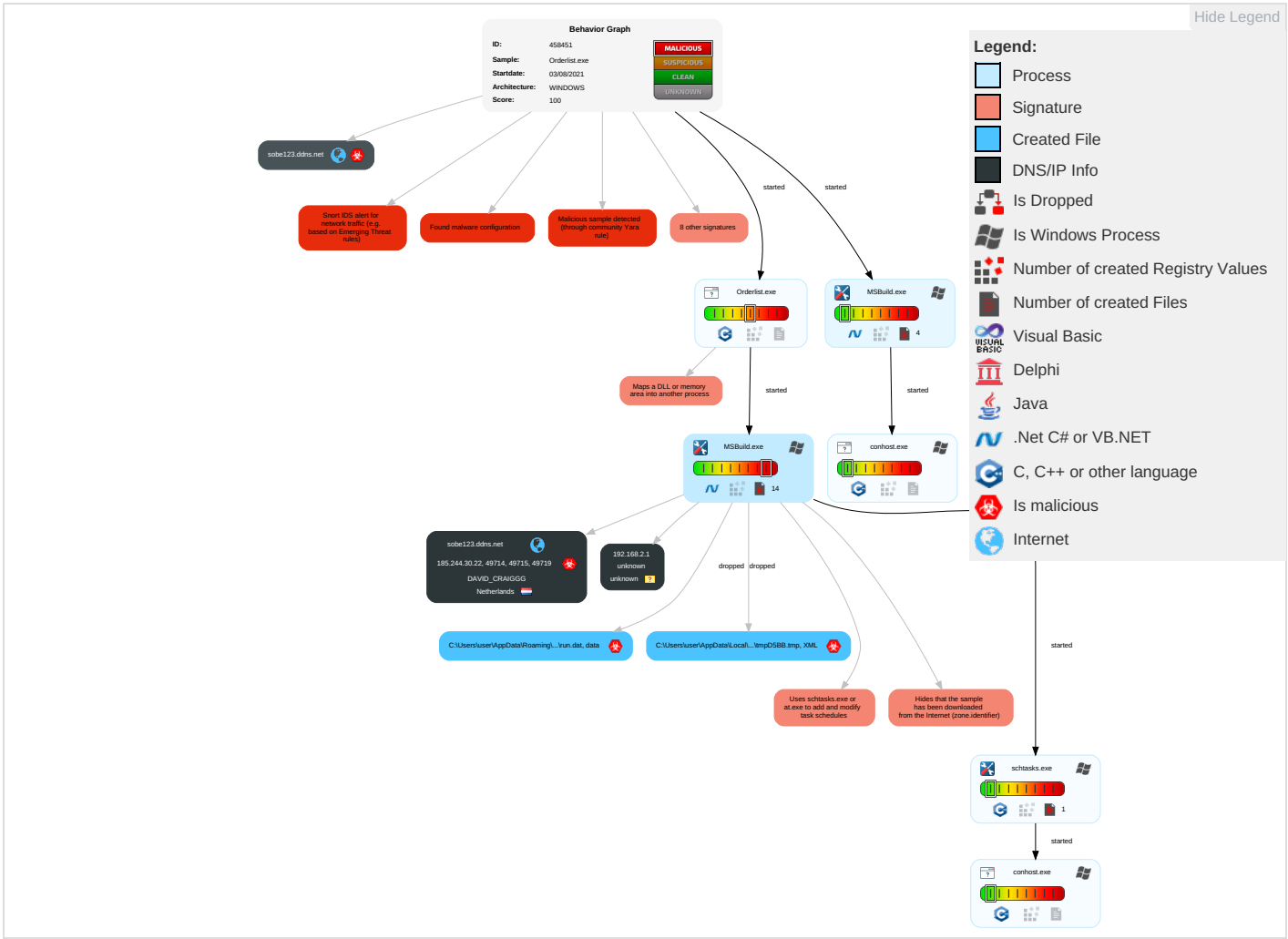
- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eavesc Insecu Netwo Comm
Default Accounts	Command and Scripting Interpreter 2	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 3	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redire Calls/S
Domain Accounts	Scheduled Task/Job 1	Logon Script (Windows)	Logon Script (Windows)	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	Exploit Track I Locatic
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2	Manipu Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammi Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1	DCSync	System Information Discovery 2 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access

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
Orderlist.exe	26%	ReversingLabs	Win32.Backdoor.NanoBot	
Orderlist.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Orderlist.exe.37e0000.1.unpack	100%	Avira	TR/Patched.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
127.0.0.1	0%	Avira URL Cloud	safe	
sobe123.ddns.net	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sobe123.ddns.net	185.244.30.22	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
127.0.0.1	true	• Avira URL Cloud: safe	unknown
sobe123.ddns.net	true	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.244.30.22	sobe123.ddns.net	Netherlands		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458451
Start date:	03.08.2021
Start time:	11:33:46
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Orderlist.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:	30
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@8/9@20/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 98.5% (good quality ratio 90.6%) • Quality average: 79.4% • Quality standard deviation: 31%
HCA Information:	• Successful, ratio: 75% • 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
11:34:45	API Interceptor	972x Sleep call for process: MSBuild.exe modified
11:34:46	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.244.30.22	Orderpdf.exe	Get hash	malicious	Browse	
	Permintaan Baru 0010.exe	Get hash	malicious	Browse	
	Shipping document PL and BL0070,pdf.exe	Get hash	malicious	Browse	
	Shipping document PL and BL0070,pdf.exe	Get hash	malicious	Browse	
	Shipping document PL and BL0070,pdf.exe	Get hash	malicious	Browse	
	AWB 686553534 L#U00f4 h#U00e0ng ,pdf.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sobe123.ddns.net	Orderpdf.exe	Get hash	malicious	Browse	• 185.244.30.22

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	Orderpdf.exe	Get hash	malicious	Browse	• 185.244.30.22
	d1IaoX0mpm.exe	Get hash	malicious	Browse	• 185.140.53.6
	ORDER LIST.xlsx	Get hash	malicious	Browse	• 185.140.53.6
	8146Q5rN9g.exe	Get hash	malicious	Browse	• 91.193.75.162
	Scanned Documents 001.doc	Get hash	malicious	Browse	• 91.193.75.162
	Quotation Request August RFQ8012021.exe	Get hash	malicious	Browse	• 185.140.53.253
	NEW PO pdf.exe	Get hash	malicious	Browse	• 91.193.75.162
	Permintaan Baru 0010.exe	Get hash	malicious	Browse	• 185.244.30.22
	5yvgVnT8wz.exe	Get hash	malicious	Browse	• 185.244.30.23
	LxYbtlP5nB.exe	Get hash	malicious	Browse	• 185.244.30.23
	eInFMnZWWV.exe	Get hash	malicious	Browse	• 185.244.30.143

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Purchase order FOD-0056-2021-D.exe	Get hash	malicious	Browse	• 91.193.75.162
	ARRIVAL NOTICE FOR NEW ORDER190009.exe	Get hash	malicious	Browse	• 185.140.53.142
	Quotation RequestQR28072021.exe	Get hash	malicious	Browse	• 185.140.53.253
	Spare Parts Requisition-003,004.exe	Get hash	malicious	Browse	• 185.244.30.238
	Order List.exe	Get hash	malicious	Browse	• 91.193.75.228
	Quote 992002892.doc	Get hash	malicious	Browse	• 185.244.30.238
	4FNiWwUTLR.exe	Get hash	malicious	Browse	• 185.244.30.238
	PMA21-110.exe	Get hash	malicious	Browse	• 91.193.75.228
	PEDIDO DE COMPRA ASHCROFT - 41901E-001,pdf.exe	Get hash	malicious	Browse	• 185.140.53.11

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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:Q3LadLCR22IAQykdL1tZbLsbFLIP12MUAvvro6ysGMFLIP12MUAvvrs:Q3LaJU20NaL1tZbgbe4MqJsGMe4M6
MD5:	65CE98936A67552310EFE2F0FF5BDF88
SHA1:	8133653A6B9A169C7496ADE315CED322CFC3613A
SHA-256:	682F7C55B1B6E189D17755F74959CD08762F91373203B3B982ACFFCADE2E871A
SHA-512:	2D00AC024267EC384720A400F6D0B4F7EDDF49FAF8AB3C9E6CBFBBAE90ECADACA9022B33E3E8EC92E4F57C7FC830299C8643235EB4AA7D8A6AFE9DD1775F57C3
Malicious:	false
Reputation:	moderate, very likely benign file
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\Temp\tmpD5BB.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**
Reputation:	moderate, very likely benign file
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):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhDjhL
MD5:	2CC2E05CB39A76B255530F61BA4AA2E3
SHA1:	76BD6001B1922B2B3FB2F618740FA74A6C532A7F
SHA-256:	FBF89196FF1A9FC33EE6C42DC0A959DAA89E2322F3417C77534C9968C0885271
SHA-512:	2EACD3A81456781803A9C14F7471DBBDB126BBE7AEC3105B1A49AB115A8BB831EA0D1DF48BAB00EB8231B114EAE5A03DF73A7A60B45BA03CB2F92382CF4DB B38
Malicious:	false
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.....[.&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.....[.&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.....[.&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.....[.&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:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:z5Tt:Vh
MD5:	5AE21F9EFD353DB4655E78BF1D985A51
SHA1:	BE4FA7084E270D516D19CB9FD57DEFDC51407AD0
SHA-256:	9FA1633CB2F77A3059A545A5C99CDB30E669304A050DCA66F79308423575FF94
SHA-512:	B84F1CB9B768B92543C4847E4E6E863AB59D0F676E09A2A6B0BB550695208CB8DAF9801678A7DBDC2E4F41A363E0AF018B1F505F7840D5A5FD77E69EF8F6D34 C
Malicious:	**true**
Preview:	..+\.V.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	24
Entropy (8bit):	4.584962500721156
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBn:RzWDqTB
MD5:	3FCC766D28BFD974C68B38C27D0D7A9A
SHA1:	45ED19A78D9B79E46EDBFC3E3CA58E90423A676B
SHA-256:	39A25F1AB5099005A74CF04F3C61C3253CD9BDA73B85228B58B45AAA4E838641
SHA-512:	C7D47BDAABEEBB8C9D9B31CC4CE968EAF291771762FA022A2F55F9BA4838E71FDBD3F83792709E47509C5D94629D6D274CC933371DC01560D13016D944012D 5
Malicious:	false
Preview:	9iH...}Z.4..f.....l.d

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.425704882778696
Encrypted:	false
SSDEEP:	3:9bzY6oRDJoTBPcgY6oRDMjmPl:RzWDqTdRWDMCd
MD5:	CA214D2E41394F5ADA74FA4F2EA15CB5
SHA1:	32E3F863838177349F2AF70CA1CE695B3C184166
SHA-256:	B6E370AF3F5C1001C79BC19706D1A5B1803C59BC45AEFAB4BD18FC67034F47A1
SHA-512:	E9C268BCDE8872F4DD2964ACA6F9C51834E42E2AF7FF2E1C327573CEDC98127B0EDBBF8E76E456FFF82A28FC46A210D91EEEA2242ECED5368D107436B3492C 14

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Malicious:	false
Preview:	9iH...}Z.4..f.....l.d9iH...}Z.4..f..... 8.j....|.&X..e.F.*.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	426832
Entropy (8bit):	**7.999527918131335**
Encrypted:	**true**
SSDEEP:	6144:zKfHbamD8WN+JQYrjM7Ei2CsFJjyh9zvgPonV5HqZcPVT4Eb+Z6no3QSzjeMsdF/:zKf137EiDsTjevgArYcPVLoTQS+0iv
MD5:	653DDDCB6C89F6EC51F3DDC0053C5914
SHA1:	4CF7E7D42495CE01C261E4C5C4B8BF6CD76CCEE5
SHA-256:	83B9CAE66800C768887FB270728F6806CBEBDEAD9946FA730F01723847F17FF9
SHA-512:	27A467F2364C21CD1C6C34EF1CA5FFB09B4C3180FC9C025E293374EB807E4382108617BB4B97F8EBBC27581CD6E5988BB5E21276B3CB829C1C0E49A6FC9463A
Malicious:	false
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!..;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

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
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe

\Device\ConDrv	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	235
Entropy (8bit):	5.107306146099542
Encrypted:	false
SSDEEP:	6:zx3M1tlAX8bSWR30qysGMQbSVRRZBXVRbJ0fFPRAgRYan:zK1XnV30ZsGMIG9BFRbQ5AUYan
MD5:	67DDD8252A246E7B14649B0063E351C0
SHA1:	AAE1C6839D1CC4A626D0FB2D4773823AD209FA17
SHA-256:	24C8283BA3F7FCA2E4CEF6F141263DD1E8A36E5A5CD96A97BFE83525D7663116
SHA-512:	326A5E0A440F60D4808C91499F1F3616C496B67DC053B4A2A40B0FE09002074AE5365018781F8746E98E7E3CFCD35F1310D17FB7C2138A8157318E6791987025
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 MSB1009: Project file does not exist...Switch: 0..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.566964052983995

General

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:	Orderlist.exe
File size:	457359
MD5:	57201aec028c2bd9a91e79ed81aeb868
SHA1:	150471c9ac6f4324bbcd1a3852d1755fed87440a
SHA256:	580eb6d5dffc61f35b4fe0ea5c0ab113af6f39e971282f9fff016b7f54d036ab
SHA512:	f7158703ec8359936dcf6a48b045d0b427f594dc0dd5daed66d043ccb696debe0bf44b7861de23903220359ea074478102601203f74d82c7439549bd97116828
SSDEEP:	12288:0NmRAtaiaYtrH398p37jUSDNlXPn66tVhP9Cx:0Nm6nHN8pLjUSppn6eQx
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....a9.p.j.p.j.p.j...k.p.j...k.p.j...k.p.j...k.p.j...k.p.j...k.p.j.p.j.p.j...k.p.j...j.p.j.p.j.p.j...k.p.jRich.p.j.....

File Icon

Icon Hash:	10ecd4d2d8cce400

Static PE Info

General

Entrypoint:	0x40187e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x6108F2D1 [Tue Aug 3 07:40:01 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:	47132e7294d9df76f8ee6d6805dd5e2d

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xb0b4	0xb200	False	0.589339009831	data	6.61597401291	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xd000	0x5a08	0x5c00	False	0.414996603261	data	4.86737104146	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x13000	0x1b24	0x1000	False	0.2392578125	data	2.69306515191	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x15000	0xb4	0x200	False	0.205078125	data	0.920266383871	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x16000	0x29388	0x29400	False	0.0764678030303	data	3.16536919122	IMAGE_SCN_CNT_INITIALIZED_DATA, 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
08/03/21-11:34:46.556393	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	5656	192.168.2.5	185.244.30.22
08/03/21-11:34:52.608063	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49715	5656	192.168.2.5	185.244.30.22
08/03/21-11:34:59.093082	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49719	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:05.122589	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:11.198158	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49723	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:19.298793	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:25.306945	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49725	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:31.535213	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:37.723027	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:44.442768	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:50.943540	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	5656	192.168.2.5	185.244.30.22
08/03/21-11:35:57.169057	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	5656	192.168.2.5	185.244.30.22
08/03/21-11:36:04.419421	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	5656	192.168.2.5	185.244.30.22
08/03/21-11:36:10.588078	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49751	5656	192.168.2.5	185.244.30.22
08/03/21-11:36:16.760728	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49752	5656	192.168.2.5	185.244.30.22
08/03/21-11:36:22.878749	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	5656	192.168.2.5	185.244.30.22
08/03/21-11:36:28.835778	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	5656	192.168.2.5	185.244.30.22
08/03/21-11:36:34.868021	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	5656	192.168.2.5	185.244.30.22
08/03/21-11:36:40.949402	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	5656	192.168.2.5	185.244.30.22
08/03/21-11:36:46.919926	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	5656	192.168.2.5	185.244.30.22

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 11:34:46.300275087 CEST	192.168.2.5	8.8.8.8	0x7b0e	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:34:52.439148903 CEST	192.168.2.5	8.8.8.8	0xb04a	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:34:58.911879063 CEST	192.168.2.5	8.8.8.8	0xd65	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:04.963385105 CEST	192.168.2.5	8.8.8.8	0x8673	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:11.048209906 CEST	192.168.2.5	8.8.8.8	0xa298	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:19.131186962 CEST	192.168.2.5	8.8.8.8	0xde5e	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:25.141386986 CEST	192.168.2.5	8.8.8.8	0xd66e	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:31.373980999 CEST	192.168.2.5	8.8.8.8	0x70da	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:37.551378012 CEST	192.168.2.5	8.8.8.8	0x53a0	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:44.286135912 CEST	192.168.2.5	8.8.8.8	0x8f61	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:50.717076063 CEST	192.168.2.5	8.8.8.8	0x13fb	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:56.923703909 CEST	192.168.2.5	8.8.8.8	0xe1db	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:04.220123053 CEST	192.168.2.5	8.8.8.8	0x7ff8	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:10.335843086 CEST	192.168.2.5	8.8.8.8	0x282d	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:16.592588902 CEST	192.168.2.5	8.8.8.8	0xcf9b	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:22.705518007 CEST	192.168.2.5	8.8.8.8	0xccc2	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:28.675108910 CEST	192.168.2.5	8.8.8.8	0xc211	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:34.704138994 CEST	192.168.2.5	8.8.8.8	0x6614	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:40.767715931 CEST	192.168.2.5	8.8.8.8	0xc7b1	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:46.760056973 CEST	192.168.2.5	8.8.8.8	0x6d01	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 11:34:46.335510015 CEST	8.8.8.8	192.168.2.5	0x7b0e	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:34:52.474721909 CEST	8.8.8.8	192.168.2.5	0xb04a	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:34:58.948497057 CEST	8.8.8.8	192.168.2.5	0xd65	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:04.996550083 CEST	8.8.8.8	192.168.2.5	0x8673	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:11.072742939 CEST	8.8.8.8	192.168.2.5	0xa298	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:19.163836002 CEST	8.8.8.8	192.168.2.5	0xde5e	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:25.179255009 CEST	8.8.8.8	192.168.2.5	0xd66e	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:31.407829046 CEST	8.8.8.8	192.168.2.5	0x70da	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 11:35:37.578969955 CEST	8.8.8.8	192.168.2.5	0x53a0	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:44.318723917 CEST	8.8.8.8	192.168.2.5	0x8f61	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:50.754591942 CEST	8.8.8.8	192.168.2.5	0x13fb	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:35:56.957531929 CEST	8.8.8.8	192.168.2.5	0xe1db	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:04.254407883 CEST	8.8.8.8	192.168.2.5	0x7ff8	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:10.369540930 CEST	8.8.8.8	192.168.2.5	0x282d	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:16.628025055 CEST	8.8.8.8	192.168.2.5	0xcf9b	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:22.741219044 CEST	8.8.8.8	192.168.2.5	0xccc2	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:28.707896948 CEST	8.8.8.8	192.168.2.5	0xc211	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:34.739733934 CEST	8.8.8.8	192.168.2.5	0x6614	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:40.800370932 CEST	8.8.8.8	192.168.2.5	0xc7b1	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 11:36:46.793041945 CEST	8.8.8.8	192.168.2.5	0x6d01	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Orderlist.exe PID: 5836 Parent PID: 5636

General

Start time:	11:34:38
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Orderlist.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orderlist.exe'
Imagebase:	0x400000
File size:	457359 bytes
MD5 hash:	57201AEC028C2BD9A91E79ED81AEB868
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: 00000001.00000002.236917800.0000000003850000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.236917800.0000000003850000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.236917800.0000000003850000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.236917800.0000000003850000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: MSBuild.exe PID: 5796 Parent PID: 5836

General

Start time:	11:34:39
Start date:	03/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orderlist.exe'
Imagebase:	0xad0000
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 Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 1628 Parent PID: 5796

General

Start time:	11:34:44
Start date:	03/08/2021
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\tmpD5BB.tmp'
Imagebase:	0x12e0000
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: 1324 Parent PID: 1628

General

Start time:	11:34:44
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: 4204 Parent PID: 904

General

Start time:	11:34:46
Start date:	03/08/2021
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:	0x890000
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: 1188 Parent PID: 4204

General

Start time:	11:34:46
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false

Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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