ID: 458217
Sample Name: Orderpdf.exe
Cookbook: default.jbs
Time: 03:31:10
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

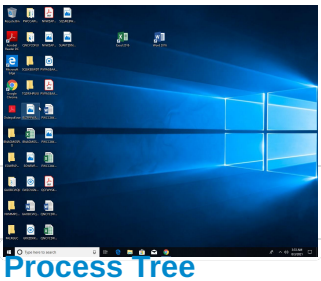
Windows Analysis Report Orderpdf.exe

Overview

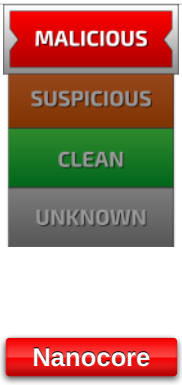
General Information

Sample Name:	Orderpdf.exe
Analysis ID:	458217
MD5:	2849c98c8d0712..
SHA1:	2431f573d98aaaa.
SHA256:	959536bfd1cf197..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



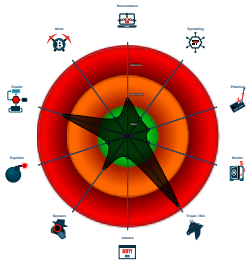
Nanocore

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**
- Orderpdf.exe (PID: 1268 cmdline: 'C:\Users\user\Desktop\Orderpdf.exe' MD5: 2849C98C8D071260B2618BEACF873A98)
  - MSBuild.exe (PID: 5876 cmdline: 'C:\Users\user\Desktop\Orderpdf.exe' MD5: 88BBB7610152B48C2B3879473B17857E)
    - schtasks.exe (PID: 4436 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp86BE.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 6004 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\MSBuild.exe 0 MD5: 88BBB7610152B48C2B3879473B17857E)
  - conhost.exe (PID: 6076 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
00000000.00000002.205053043.000000000212 0000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.205053043.000000000212 0000.00000040.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
00000000.00000002.205053043.000000000212 0000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.205053043.000000000212 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: Orderpdf.exe PID: 1268	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x70948:$x1: NanoCore.ClientPluginHost • 0x70985:$x2: IClientNetworkHost • 0x74476:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0x7f4e4:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.Orderpdf.exe.2120000.1.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.Orderpdf.exe.2120000.1.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0.2.Orderpdf.exe.2120000.1.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.Orderpdf.exe.2120000.1.raw.unpack	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:$j: #=q
0.2.Orderpdf.exe.2120000.1.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
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:

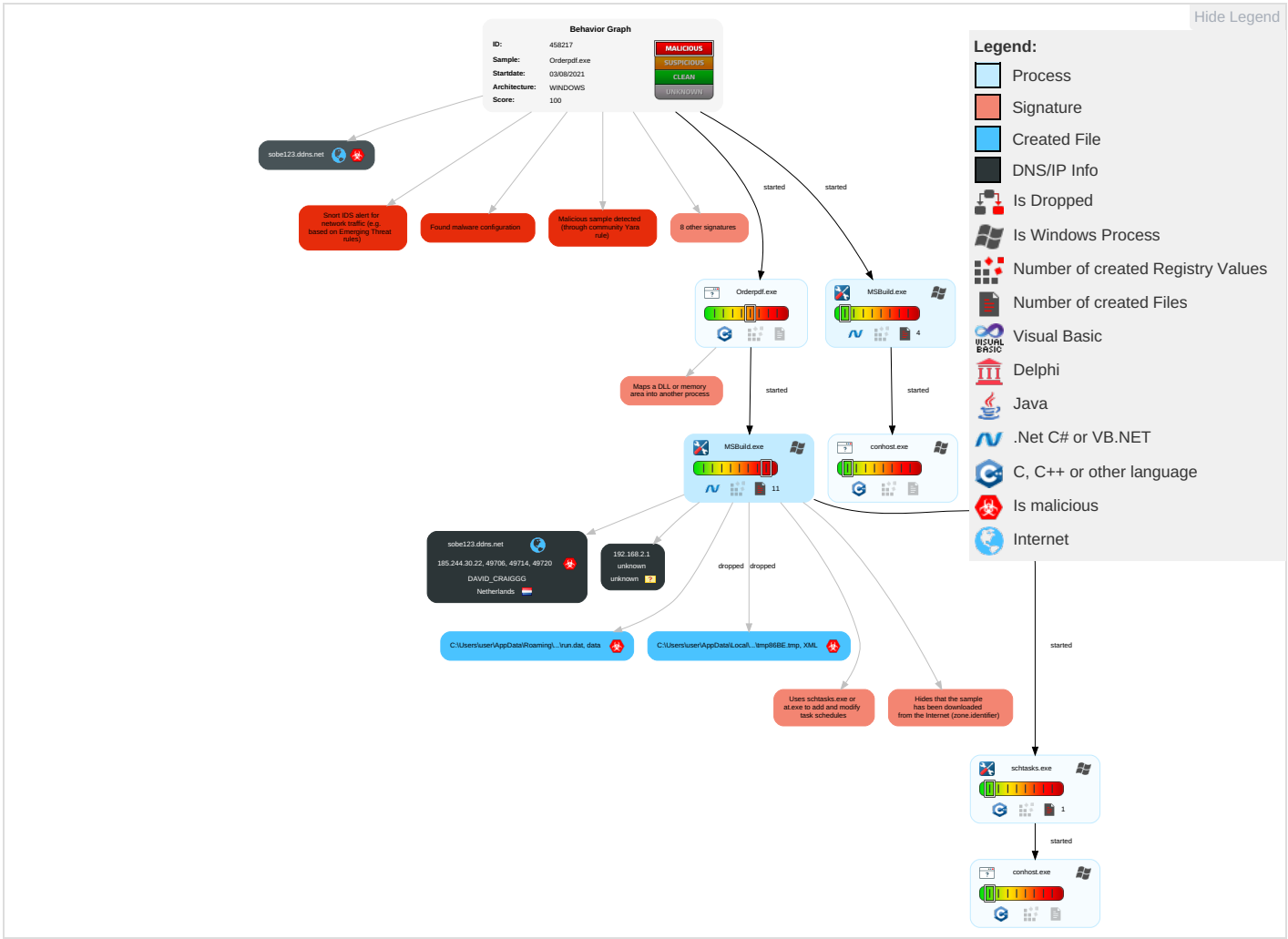
- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 2	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	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	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 SS7 Track Devic Location
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 Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 2 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir

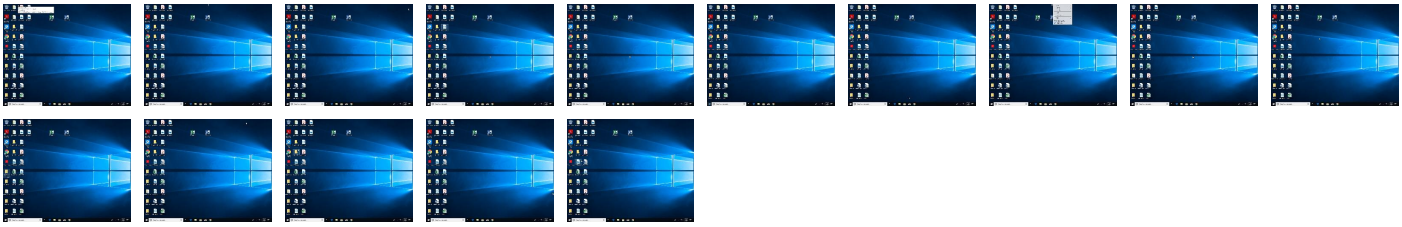
Behavior Graph



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
Orderpdf.exe	28%	Virustotal		Browse
Orderpdf.exe	22%	ReversingLabs	Win32.Trojan.NanoBot	
Orderpdf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
127.0.0.1	0%	Virustotal		Browse
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	• 0%, Virustotal, Browse • 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:	458217
Start date:	03.08.2021
Start time:	03:31:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Orderpdf.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:	33
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@8/6@20/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 67% • 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
03:32:00	API Interceptor	1064x Sleep call for process: MSBuild.exe modified
03:32:02	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	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

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	d1laoX0mpm.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
	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

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	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
	Quotation.exe	Get hash	malicious	Browse	• 185.244.30.53

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\tmp86BE.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

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

Size (bytes):	2320
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhDjhDjhL
MD5:	2CC2E05CB39A76B255530F61BA4AA2E3
SHA1:	76BD6001B1922B2B3FB2F618740FA74A6C532A7F
SHA-256:	FBF89196FF1A9FC33EE6C42DC0A959DAA89E2322F3417C77534C9968C0885271
SHA-512:	2EACD3A81456781803A9C14F7471DBBDB126BBE7AEC3105B1A49AB115A8BB831EA0D1DF48BAB00EB8231B114EAE5A03DF73A7A60B45BA03CB2F92382CF4DB B38
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......[.&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:	3:6vtn:6vt
MD5:	604254C4E0DED10AC094C2AEFF16A952
SHA1:	D0CCCC461EE99F9C1D7DE9045FEBE2BB8753597C
SHA-256:	9C14AE70F96EB4C5BCCADA9E26DE13EB95ED53E08D10F2283F51049A3381E5E9
SHA-512:	14229C84CA48525291DE039DC041A053ABAEBCFA17E7A351A36CC8BF06971A2A4CBC77DB5E4B019918961F2790AD4C63946A26A5240066924C06539C9CAD639
Malicious:	**true**
Reputation:	low
Preview:	....iV.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
Malicious:	false
Reputation:	moderate, very likely benign file
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

\Device\ConDrv	
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):	6.186849273906373
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:	Orderpdf.exe
File size:	869938
MD5:	2849c98c8d071260b2618beacf873a98
SHA1:	2431f573d98aaaaa1752b73c4a5f53e8b4660e50
SHA256:	959536bfd1cf19758dde804eaf7e1d38585b573ccf4dc327898979f29cac33a8
SHA512:	0e84db59a75e6010953f247e74716996f7c652d7b9a541cd3407aa5284958c17c7cb3750d638240410feaea4804fe5d700fc4303eb0f18a5b96ef1833553efab
SSDEEP:	12288:f1Wl8T5UM63xjmelf+6QY+IffW3TLueA0b:fA2adx06QYffaLNb
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....;$G..E)].E)].E)]k.*\kE)]k.,\.E)]k.-\eE)]D.*\kE)]D.,\DE)]D.-\]E)]k.(\vE)].E(].E)]..,\vE)]...]~E)].E.]~E)]..+\~E)]Rich.E)].....

File Icon

Icon Hash:	00ecf0f0e8ecf400

Static PE Info

General

Entrypoint:	0x420e4a
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:	0x61087E6E [Mon Aug 2 23:23:26 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:	49be0836dac021f86af2cb207b4613c8

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x34912	0x34a00	False	0.446050141033	data	6.54583953865	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x36000	0x408b6	0x40a00	False	0.257729388298	data	4.10647165512	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x77000	0x1e08	0x1000	False	0.296630859375	DOS executable (COM)	3.39752271911	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x79000	0x150	0x200	False	0.33203125	data	1.72024643613	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.tls	0x7a000	0x9	0x200	False	0.033203125	data	0.0203931352361	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x7b000	0x294e0	0x29600	False	0.0884688916163	data	3.29281992913	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
08/03/21-03:32:01.658714	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	5656	192.168.2.3	185.244.30.22
08/03/21-03:32:07.884442	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	5656	192.168.2.3	185.244.30.22
08/03/21-03:32:13.096068	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	5656	192.168.2.3	185.244.30.22
08/03/21-03:32:20.053138	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49726	5656	192.168.2.3	185.244.30.22
08/03/21-03:32:26.158381	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	5656	192.168.2.3	185.244.30.22
08/03/21-03:32:35.527911	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	5656	192.168.2.3	185.244.30.22
08/03/21-03:32:41.635368	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49732	5656	192.168.2.3	185.244.30.22
08/03/21-03:32:48.089965	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49733	5656	192.168.2.3	185.244.30.22
08/03/21-03:32:56.068267	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:02.446681	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:08.692026	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49744	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:14.889582	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:21.077319	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49746	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:27.201337	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:33.527958	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	5656	192.168.2.3	185.244.30.22

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-03:33:40.158463	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:46.612650	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:52.859023	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49757	5656	192.168.2.3	185.244.30.22
08/03/21-03:33:58.969834	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49758	5656	192.168.2.3	185.244.30.22
08/03/21-03:34:04.972456	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	5656	192.168.2.3	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 03:32:01.459546089 CEST	192.168.2.3	8.8.8.8	0xae9c	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:07.727443933 CEST	192.168.2.3	8.8.8.8	0x275a	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:12.893038988 CEST	192.168.2.3	8.8.8.8	0x328c	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:19.907943010 CEST	192.168.2.3	8.8.8.8	0x17e8	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:26.012536049 CEST	192.168.2.3	8.8.8.8	0xd834	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:32.371571064 CEST	192.168.2.3	8.8.8.8	0xa93a	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:41.492619038 CEST	192.168.2.3	8.8.8.8	0x37d6	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:47.952207088 CEST	192.168.2.3	8.8.8.8	0x6a52	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:55.367870092 CEST	192.168.2.3	8.8.8.8	0x3950	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:02.150737047 CEST	192.168.2.3	8.8.8.8	0xae82	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:08.559366941 CEST	192.168.2.3	8.8.8.8	0x8027	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:14.747713089 CEST	192.168.2.3	8.8.8.8	0xae74	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:20.908586025 CEST	192.168.2.3	8.8.8.8	0x8775	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:27.059242964 CEST	192.168.2.3	8.8.8.8	0x79c9	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:33.388942957 CEST	192.168.2.3	8.8.8.8	0x39f4	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:39.841692924 CEST	192.168.2.3	8.8.8.8	0xdd75	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:46.470058918 CEST	192.168.2.3	8.8.8.8	0xf814	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:52.714616060 CEST	192.168.2.3	8.8.8.8	0xb9c8	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:58.801398039 CEST	192.168.2.3	8.8.8.8	0xa220	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 03:34:04.816489935 CEST	192.168.2.3	8.8.8.8	0xfaa0	Standard query (0)	sobe123.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

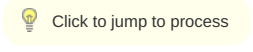
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 03:32:01.494106054 CEST	8.8.8.8	192.168.2.3	0xae9c	No error (0)	sobe123.ddns.net		185.244.30.22	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 03:32:07.762829065 CEST	8.8.8.8	192.168.2.3	0x275a	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:12.928888083 CEST	8.8.8.8	192.168.2.3	0x328c	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:19.943284988 CEST	8.8.8.8	192.168.2.3	0x17e8	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:26.048392057 CEST	8.8.8.8	192.168.2.3	0xd834	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:32.403898954 CEST	8.8.8.8	192.168.2.3	0xa93a	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:41.526473045 CEST	8.8.8.8	192.168.2.3	0x37d6	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:47.976875067 CEST	8.8.8.8	192.168.2.3	0x6a52	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:32:55.394695997 CEST	8.8.8.8	192.168.2.3	0x3950	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:02.184956074 CEST	8.8.8.8	192.168.2.3	0xae82	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:08.584351063 CEST	8.8.8.8	192.168.2.3	0x8027	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:14.780982971 CEST	8.8.8.8	192.168.2.3	0xae74	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:20.944596052 CEST	8.8.8.8	192.168.2.3	0x8775	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:27.093126059 CEST	8.8.8.8	192.168.2.3	0x79c9	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:33.421489954 CEST	8.8.8.8	192.168.2.3	0x39f4	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:39.878473043 CEST	8.8.8.8	192.168.2.3	0xdd75	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:46.502367020 CEST	8.8.8.8	192.168.2.3	0xf814	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:52.748580933 CEST	8.8.8.8	192.168.2.3	0xb9c8	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:33:58.836028099 CEST	8.8.8.8	192.168.2.3	0xa220	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)
Aug 3, 2021 03:34:04.851423025 CEST	8.8.8.8	192.168.2.3	0xfaa0	No error (0)	sobe123.dd ns.net		185.244.30.22	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Orderpdf.exe PID: 1268 Parent PID: 5648

General

Start time:	03:31:57
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Orderpdf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Orderpdf.exe'
Imagebase:	0x400000
File size:	869938 bytes
MD5 hash:	2849C98C8D071260B2618BEACF873A98
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: 00000000.00000002.205053043.0000000002120000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000000.00000002.205053043.0000000002120000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.205053043.0000000002120000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.205053043.0000000002120000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: MSBuild.exe PID: 5876 Parent PID: 1268

General

Start time:	03:31:57
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\Orderpdf.exe'
Imagebase:	0xd90000
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: 4436 Parent PID: 5876

General

Start time:	03:31:59
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\tmp86BE.tmp'
Imagebase:	0x1240000
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: 1636 Parent PID: 4436

General

Start time:	03:32:00
Start date:	03/08/2021
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: 6004 Parent PID: 528

General

Start time:	03:32:02
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:	0x6d0000
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: 6076 Parent PID: 6004

General

Start time:	03:32:02
Start date:	03/08/2021
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