ID: 457798
Sample Name: Order List.exe
Cookbook: default.jbs
Time: 10:36:10
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

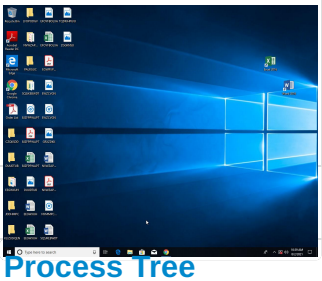
Windows Analysis Report Order List.exe

Overview

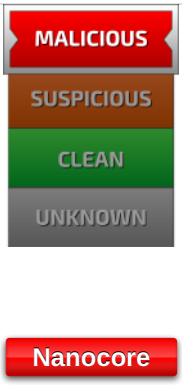
General Information

Sample Name:	Order List.exe
Analysis ID:	457798
MD5:	e2893188b7e7d6..
SHA1:	6a7a3d1ecb2175..
SHA256:	09b6f40cf52bde3..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



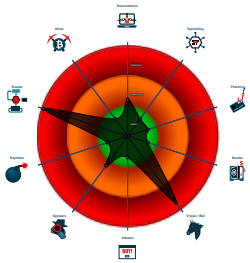
Nanocore

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

Signatures

- Detected Nanocore Rat
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code references suspic…
- C2 URLs / IPs found in malware con…

Classification



Process Tree

- **System is w10x64**
- Order List.exe (PID: 5776 cmdline: 'C:\Users\user\Desktop\Order List.exe' MD5: E2893188B7E7D6F19581A7981C2A0A75)
  - schtasks.exe (PID: 1848 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AylDGlu' /XML 'C:\Users\user\AppData\Local\Temp\tmp5BCE.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 5564 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
  - MSBuild.exe (PID: 4988 cmdline: {path} MD5: D621FD77BD585874F9686D3A76462EF1)
    - schtasks.exe (PID: 3100 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor' /xml 'C:\Users\user\AppData\Local\Temp\tmp6DFE.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 4692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5512 cmdline: 'schtasks.exe' /create /f /tn 'DHCP Monitor Task' /xml 'C:\Users\user\AppData\Local\Temp\tmp71A9.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 1716 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- MSBuild.exe (PID: 488 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe 0 MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 1012 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5276 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0 MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 5284 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 6080 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: D621FD77BD585874F9686D3A76462EF1)
  - conhost.exe (PID: 3980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "1b30e380-3e9d-40b0-8d35-d1fb4c64",
  "Group": "gintx$$",
  "Domain1": "79.134.225.115",
  "Domain2": "gintex.ddns.net",
  "Port": 21180,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4",
  "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
00000012.00000002.504687984.0000000006E1 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x350b:$x1: NanoCore.ClientPluginHost • 0x3525:$x2: IClientNetworkHost
00000012.00000002.504687984.0000000006E1 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x350b:$x2: NanoCore.ClientPluginHost • 0x52b6:$s4: PipeCreated • 0x34f8:$s5: IClientLoggingHost
00000012.00000002.504506508.0000000006D9 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x16e3:$x1: NanoCore.ClientPluginHost • 0x171c:$x2: IClientNetworkHost
00000012.00000002.504506508.0000000006D9 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x16e3:$x2: NanoCore.ClientPluginHost • 0x1800:$s4: PipeCreated • 0x16fd:$s5: IClientLoggingHost
00000012.00000002.500969666.0000000003FD 6000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x30da:$a: NanoCore • 0x313b:$a: NanoCore • 0x317e:$a: NanoCore • 0x31be:$a: NanoCore • 0x33fa:$a: NanoCore • 0x349a:$a: NanoCore • 0x3c72:$a: NanoCore • 0x4265:$a: NanoCore • 0x43b6:$a: NanoCore • 0x5210:$a: NanoCore • 0x5477:$a: NanoCore • 0x548c:$a: NanoCore • 0x54ab:$a: NanoCore • 0xe3ae:$a: NanoCore • 0xe3d7:$a: NanoCore • 0x3150:$b: ClientPlugin • 0x3403:$b: ClientPlugin • 0x34a3:$b: ClientPlugin • 0xe1ce:$b: ClientPlugin • 0xe1e2:$b: ClientPlugin • 0xe212:$b: ClientPlugin

Click to see the 43 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
18.2.MSBuild.exe.6df0000.29.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3d99:$x1: NanoCore.ClientPluginHost • 0x3db3:$x2: IClientNetworkHost
18.2.MSBuild.exe.6df0000.29.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3d99:$x2: NanoCore.ClientPluginHost • 0x4dce:$s4: PipeCreated • 0x3d86:$s5: IClientLoggingHost
18.2.MSBuild.exe.6da0000.24.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x5b0b:$x1: NanoCore.ClientPluginHost • 0x5b44:$x2: IClientNetworkHost
18.2.MSBuild.exe.6da0000.24.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x5b0b:$x2: NanoCore.ClientPluginHost • 0x5c0f:$s4: PipeCreated • 0x5b25:$s5: IClientLoggingHost
18.2.MSBuild.exe.3fde83e.11.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3d99:$x1: NanoCore.ClientPluginHost • 0x3db3:$x2: IClientNetworkHost
Click to see the 116 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 dropped file

Yara detected Nanocore RAT

Compliance:

Detected unpacking (overwrites its own PE header)

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:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Injects a PE file into a foreign processes

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

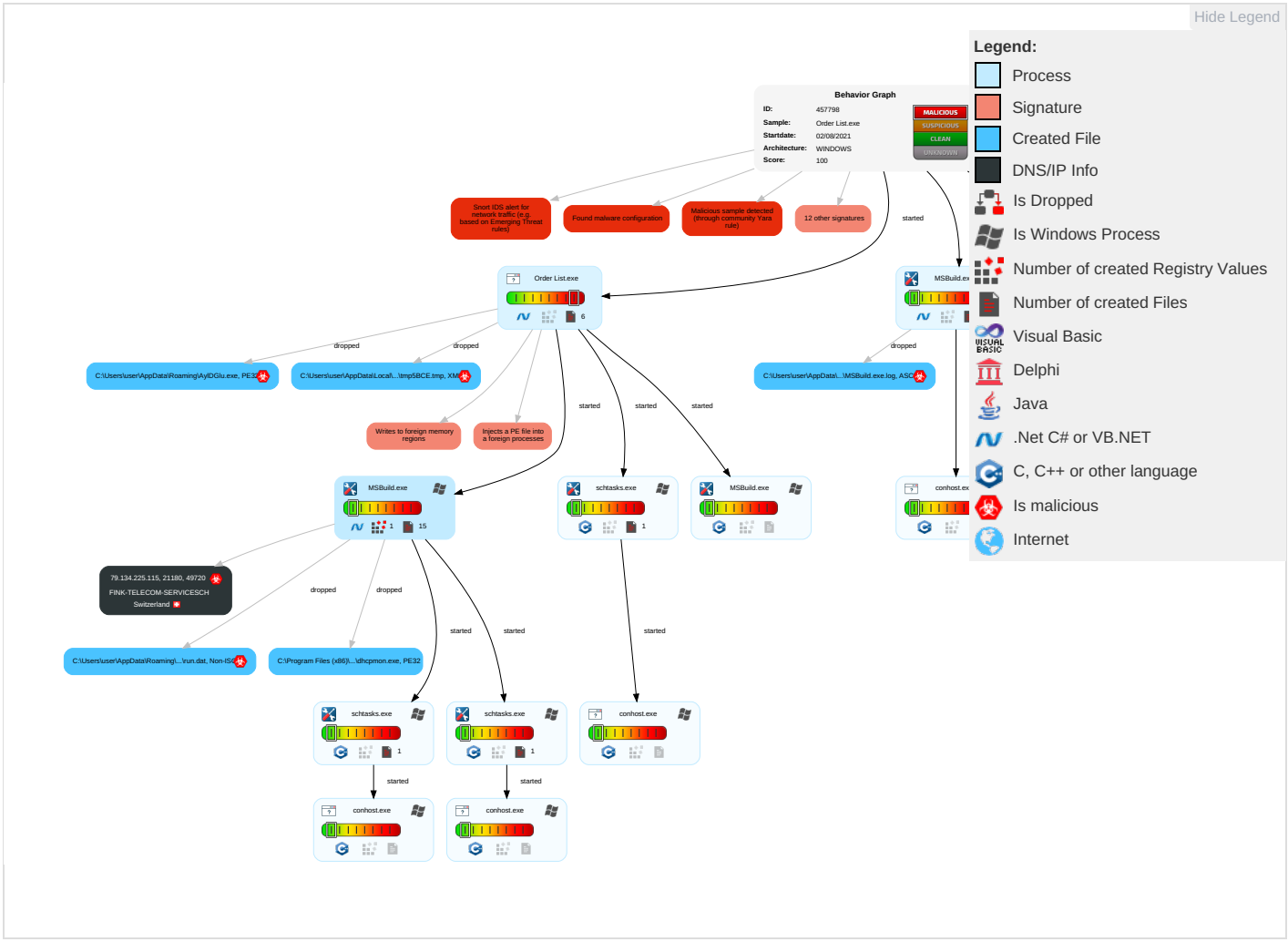
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1 1	Process Injection 2 1 1	Masquerading 2	OS Credential Dumping	Security Software Discovery 2 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eav Inse Net Con
Default Accounts	Scheduled Task/Job 1 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exp Red Call
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Virtualization/Sandbox Evasion 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exp Trac Loca
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 2 1 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mar Dev Con

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2 3	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jam Den Ser

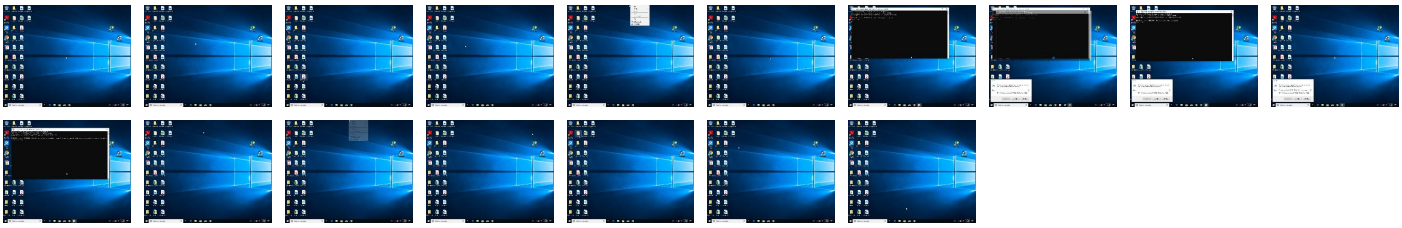
Behavior Graph



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	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\AylDGlu.exe	33%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.MSBuild.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.Order List.exe.e50000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen2		Download File
18.2.MSBuild.exe.6240000.18.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/://w	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/u_	0%	Avira URL Cloud	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlBSZeai	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnU	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/fr-f	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.urwpp.deFr	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.urwpp.depS	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
gintex.ddns.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/c_	0%	Avira URL Cloud	safe	
http://www.fontbureau.comrsiv	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.fontbureau.comtuF	0%	Avira URL Cloud	safe	
79.134.225.115	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0/j_	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/R	0%	URL Reputation	safe	
http://www.fontbureau.comFc_	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/W	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/F_var	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/-_	0%	Avira URL Cloud	safe	
http://www.urwpp.deF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/c_	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/F_var	0%	Avira URL Cloud	safe	
http://www.fontbureau.commito	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comd.F	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Norm-_	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ww.mQ_aar	0%	Avira URL Cloud	safe	
http://www.fontbureau.comituF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/al	0%	Avira URL Cloud	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.founder.com.cn/cn-	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.comce	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/j_	0%	Avira URL Cloud	safe	
http://www.fontbureau.comc_	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

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

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.115	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	457798
Start date:	02.08.2021
Start time:	10:36:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order List.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:	37
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@20/17@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 2.2% (good quality ratio 1.5%) • Quality average: 36.1% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 93% • 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
10:37:45	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe" s>$(Arg0)
10:37:48	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
10:37:49	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.115	fu.exe	Get hash	malicious	Browse	
	Purchase Order- #020521_pdf.exe	Get hash	malicious	Browse	
	MT TT103-SWIFT_PDF.exe	Get hash	malicious	Browse	
	Purchase Order-103667.pdf.exe	Get hash	malicious	Browse	
	INQ-TR-04-21-RFQ.exe	Get hash	malicious	Browse	
	PO#040221-INQ.exe	Get hash	malicious	Browse	
	MrZNctz1uR.exe	Get hash	malicious	Browse	
	168900#.exe	Get hash	malicious	Browse	
	ORDER-PO29394934.exe	Get hash	malicious	Browse	
	ORDER-PO020043.exe	Get hash	malicious	Browse	
	ORDER-9298PO3484.exe	Get hash	malicious	Browse	
	PO-ORDER20034993.exe	Get hash	malicious	Browse	
	ORDER-PURCHASE.exe	Get hash	malicious	Browse	
	1571088388.doc	Get hash	malicious	Browse	
	RFQ Acknowledgement Form-decrypted.doc	Get hash	malicious	Browse	
	RFQ NO. 1118295-decrypted.doc	Get hash	malicious	Browse	
	p.msi	Get hash	malicious	Browse	
	mbq8XJ1u9C.rtf	Get hash	malicious	Browse	
	mbq8XJ1u9C.rtf	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	RFQ 217563.exe	Get hash	malicious	Browse	• 79.134.225.116
	ORDER CONFIRMATION - 5309,pdf.exe	Get hash	malicious	Browse	• 79.134.225.76
	y7DZJshX9j.exe	Get hash	malicious	Browse	• 79.134.225.44
	SQycD6hL4Y.exe	Get hash	malicious	Browse	• 79.134.225.12
	TENDER INQUIRY REQUIREMENTS.exe	Get hash	malicious	Browse	• 79.134.225.95
	xwcTd7Kh9O.exe	Get hash	malicious	Browse	• 79.134.225.16
	RA1_20210729.exe	Get hash	malicious	Browse	• 79.134.225.98
	spworks.msi	Get hash	malicious	Browse	• 79.134.225.73
	spworks.msi	Get hash	malicious	Browse	• 79.134.225.73
	Request For Quotation.xlsx	Get hash	malicious	Browse	• 79.134.225.16
	Faktura-835382925.exe	Get hash	malicious	Browse	• 79.134.225.73
	Order List.gz.exe	Get hash	malicious	Browse	• 79.134.225.100
	doc_18000476456499946534.exe	Get hash	malicious	Browse	• 79.134.225.44
	Bh8aCXgJx4.exe	Get hash	malicious	Browse	• 79.134.225.22
	Resumen detallado del proveedor de 1302640 de solicitud de presupuesto.exe	Get hash	malicious	Browse	• 79.134.225.8
	Investment1FZELtd.exe	Get hash	malicious	Browse	• 79.134.225.35

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	KRooWcCysc.exe	Get hash	malicious	Browse	• 79.134.225.25
	Request price for partsDP35212202122000.exe	Get hash	malicious	Browse	• 79.134.225.44
	change of bank account.exe	Get hash	malicious	Browse	• 79.134.225.44
	partsDP35212202122000.exe	Get hash	malicious	Browse	• 79.134.225.44

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	allcrhfJER.exe	Get hash	malicious	Browse	
	quotation.exe	Get hash	malicious	Browse	
	HSBC.exe	Get hash	malicious	Browse	
	f026ae3a33ea7c54bcff959e9bdd2e60.exe	Get hash	malicious	Browse	
	HUMVC_039873637892OIHGDHJZ.exe	Get hash	malicious	Browse	
	HSBC Swift.exe	Get hash	malicious	Browse	
	Purchase Order.exe	Get hash	malicious	Browse	
	Contract05072157393.exe	Get hash	malicious	Browse	
	19495C90691E8B6EEF5D55D50B9D76AE6CEB5629D6C08.exe	Get hash	malicious	Browse	
	PO# 6042089404900 & PAYMENT DETAILSpdf.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	Quotation Price - Double R Trading b.v.exe	Get hash	malicious	Browse	
	QTN TECHN 80654.exe	Get hash	malicious	Browse	
	Nizi International S.A. #New Order.exe	Get hash	malicious	Browse	
	DHL Shipment Documents.exe	Get hash	malicious	Browse	
	27bd034c36964c455e2b2ad6b264561f.exe	Get hash	malicious	Browse	
	quote #2063 almaco.exe	Get hash	malicious	Browse	
	ConsoleSniffer v4.1 installer.exe	Get hash	malicious	Browse	
	jtH33Uljkz.exe	Get hash	malicious	Browse	
	quote #60123.exe	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	261728
Entropy (8bit):	6.1750840449797675
Encrypted:	false
SSDEEP:	3072:Mao0QHGUQWWimj9q/NLpj/WWqvAw2XpFU4rwOe4ubZSif02RFi/x2uv9FeP:boZTTWxxqVpqWVRXfr802biprVu
MD5:	D621FD77BD585874F9686D3A76462EF1
SHA1:	ABCAE05EE61EE6292003AABD8C80583FA49EDDA2
SHA-256:	2CA7CF7146FB8209CF3C6CECB1C5AA154C61E046DC07AFA05E8158F2C0DDE2F6
SHA-512:	2D85A81D708ECC8AF9A1273143C94DA84E632F1E595E22F54B867225105A1D0A44F918F0FAE6F1EB15ECF69D75B6F4616699776A16A2AA8B5282100FD15CA74C
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Joe Sandbox View:	• Filename: allcrhfJER.exe, Detection: malicious, Browse • Filename: quotation.exe, Detection: malicious, Browse • Filename: HSBC.exe, Detection: malicious, Browse • Filename: f026ae3a33ea7c54bcff959e9bdd2e60.exe, Detection: malicious, Browse • Filename: HUMVC_039873637892OIHGDHJZ.exe, Detection: malicious, Browse • Filename: HSBC Swift.exe, Detection: malicious, Browse • Filename: Purchase Order.exe, Detection: malicious, Browse • Filename: Contract05072157393.exe, Detection: malicious, Browse • Filename: 19495C90691E8B6EEF5D55D50B9D76AE6CEB5629D6C08.exe, Detection: malicious, Browse • Filename: PO# 6042089404900 & PAYMENT DETAILSpdf.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: Quotation Price - Double R Trading b.v.exe, Detection: malicious, Browse • Filename: QTN TECHN 80654.exe, Detection: malicious, Browse • Filename: Nizi International S.A. #New Order.exe, Detection: malicious, Browse • Filename: DHL Shipment Documents.exe, Detection: malicious, Browse • Filename: 27bd034c36964c455e2b2ad6b264561f.exe, Detection: malicious, Browse • Filename: quote #2063 almaco.exe, Detection: malicious, Browse • Filename: ConsoleSniffer v4.1 installer.exe, Detection: malicious, Browse • Filename: jtH33Uljkz.exe, Detection: malicious, Browse • Filename: quote #60123.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Z.Z.....".0..|...B.....n.... .....@.. ....`.....O.....>.....`>..... ....H.....text....z... ...|..... ..`.rsrc....>.....@...~.....@..@.relo c.....@..B.....P.....H.....8).....|.....*.{.....*v.(=....r...p({...-..+..}....*....0..%.....(....-..*....(z.....&..}.....*.*..... ...0..5.....(....-..*..-.r+..ps>...z.....i(z.....&..}.....*.*.....%.....>....(?...(....*N..(@....oA...(...*:...(B...(....*:...(C...(....**....(....*....0..G.....(.....*..(....-...}.....*.r...p(x...&.(v.....}... ...&..}.....*.*.....7.....0..f.....-.r7..ps>...z .....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MSBuild.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	841
Entropy (8bit):	5.356220854328477
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoIvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHwvEHxDqHj
MD5:	486580834B084C92AE1F3866166C9C34
SHA1:	C8EB7E1CEF55A6C9EB931487E9AA4A2098AACEDF
SHA-256:	65C5B1213E371D449E2A239557A5F250FEA1D3473A1B5C4C5FF7492085F663FB
SHA-512:	2C54B638A52AA87F47CAB50859EFF98F07DA02993A596686B5617BA99E73ABFCD104F0F33209E24AFB32E66B4B8A225D4DB2CC79631540C21E7E8C4573DFD45
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..2,"Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order List.exe.log	
Process:	C:\Users\user\Desktop\Order List.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:ML9E4Ks29E4Kx1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MxHKX9HKx1qHiYHKhQnoPtHoxHhAHKzr
MD5:	B666A4404B132B2BF6C04FBF848EB948
SHA1:	D2EFB3D43F8B8806544D3A47F7DAEE8534981739
SHA-256:	7870616D981C8C0DE9A54E7383CD035470DB20CBF75ACDF729C32889D4B6ED96
SHA-512:	00E955EE9F14CEAE07E571A8EF2E103200CF421BAE83A66ED9F9E1AA6A9F449B653EDF1BFDB662A364D58ECF9B5FE4BB69D590DB2653F2F46A09F4D47719A862
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Size (bytes):	1037
Entropy (8bit):	5.371216502395632
Encrypted:	false
SSDEEP:	24:ML9E4Ks2wKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7KvEE4xDqE4j:MxHKXwYHKhQnoPtHoxHhAHKzvKvEHxD0
MD5:	C7F28B87C2CAD111D929CB9A0FF822F8
SHA1:	C2CF9E7A3F6EFD9000FE76EBE54E4E9AE5754267
SHA-256:	D1B02C20EACF464229AB063FA947A525E2ED7772259A8F70C7205DC13599EAE6
SHA-512:	E0F35874E02AB672CFF0553A0DA0864DAB14C05733D06395E4D0C9CDFC6F445E940310F8D01E3E1B28895F636DFBC1F510E103D1C46818400BA4E7371D8F254
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..2,"Microsoft.Build.Framework, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.Build, Version=4.0.0.0, Culture=neutral,

C:\Users\user\AppData\Local\Temp\tmp5BCE.tmp	
Process:	C:\Users\user\Desktop\Order List.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1644
Entropy (8bit):	5.165156184375511
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB9tn:cbhC7ZlNQF/rydbz9I3YODOLNdq3V
MD5:	3813C1B0AF635F5B444709655B411776
SHA1:	E53CAFA0ED3C230E932B3492E6FA98305C565A14
SHA-256:	2015BA2920185ACC6B27194B623BC7211FA93BAE40C7CE73DD315B8EC016A8A2
SHA-512:	5889042C324AABC2A4FE3F089A467B63928C3D002B6B065323425EFB6A66A73F18765EC81E89D6281DA8E201F1FC8240995E4E83A03691CE61203E202DBF6212
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>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>t

C:\Users\user\AppData\Local\Temp\tmp6DFE.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.137611098420233
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0moxtn:cbk4oL600QydbQxIYODOLedq3Zoj
MD5:	3E2B26ED8B75AE83A269595180E84EF6
SHA1:	D30A0335FCCE406BCA8BA5764288235E6192F608
SHA-256:	108BE30AEB8EB31C185A39A6726F26DACBC4E4124951C61A29ADE4B7038C71EA
SHA-512:	B6981C68FCB886CC8379A068B96931B9D4F5CC5AA9BDC467E36C4168FE6C5273A2A84D8850B12C11703EC03AC6B1F1950D1E669EFCB59FC2402CE4BBA9DC0D3
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\Local\Temp\tmp71A9.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j

C:\Users\user\AppData\Local\Temp\tmp71A9.tmp	
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\AylDGlu.exe	
Process:	C:\Users\user\Desktop\Order List.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1167872
Entropy (8bit):	6.908581539026972
Encrypted:	false
SSDEEP:	12288:hMLiJXfXUy8jmk63yoPSaEwvguKt+lCNkogRbHa1U/Fnmb68bEtFqTNmqUQzBRMo:iiwSClPuKtQoWbHWl/024TN+QzrMpnm
MD5:	E2893188B7E7D6F19581A7981C2A0A75
SHA1:	6A7A3D1ECB2175B53FB98974220F15EC6A1545CF
SHA-256:	09B6F40CF52BDE38B03CBF49A02E40370914AACFE727CDA9D6D9002CCE5DEBEB
SHA-512:	E970D0693A37412F3DC0564298768C9AA105D44B5BC5017F280A7FD3A525181AF06D0404F1DED2AABF10F85B6D6812FB189323FABBFDE27BA8CC63A3B787449
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 33%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0.....>..... .....@.. ....@.....x...S.....;..... ....H.....text..... ....`.rsrc....;.....<.....@..@.reloc..... .....@..B.....H.....`.....H~.....0..<.....(.... _.73 .O.Na%..^E.....+.(..... .R..Z ..i.a+.*.0..U.....r...p. ..U. K.B.a %...^E.....C.....S...8....r...p(..... ...Z ck"|a+.....s....(....%.(.....(.... ..{.+..(.... .%.8u....r...p(....(....,. B.q.%+. .2..%&. ...Za8G....r...p(....(....,. ..J.%+. ...%&. .. {oZa8....(..... .x..8.....(....(....rC..p(....-. ..C%+. .d.f%&. ..-.Za8.....,. ....%+. .V.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
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.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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:xj:J
MD5:	8E9918AA34A4FC689DFB85A6EE58791E
SHA1:	E92F1026D08335FDC10AE043ED70C8C4ACA11E36
SHA-256:	F5BDA608F20CF1127744E7E62383FD2444872CC21ACA5C9773F346EADC4ED55E
SHA-512:	C66E7BED8D8C726607A225A88B8A7E5C1999FBA60915C9DF49F5F6140E8FC32B6481E2F041AF51DC095E17CAB4B819B42E7B47004742C7737DE6DE17ECBFB9E
Malicious:	**true**
Preview:	c.'<.U.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	80
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVnXygY6oRDT6P2bfVn1:RzWDT62DWDT621
MD5:	4315325323A62DE913E5CCD153817BCE
SHA1:	8B38155CD8ACB20BBA0C2A8AF02BFD35B15221A8
SHA-256:	E0C2085D878FDF53CD7D8F0AA9F07490802C51FC3C14A52B6FEA96AD0743C838
SHA-512:	B5036A6CD4852CEBCA86F588D94B9D58B63EB07B2F4DEBD38D5E1BE68B0BB62F82FA239673B6C08F432A28DD50E1D15773DC3738251BD2F9959F1255D72745EB
Malicious:	false
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i..........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*l..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.887726803973036
Encrypted:	false
SSDEEP:	3:oMty8WddSJ8:oMLW6C
MD5:	6ECAFC0490DAB08E4A288E0042B6B613
SHA1:	4A4529907588505FC65CC9933980CFE6E576B3D6
SHA-256:	DC5F76FBF44B3E6CDDC14EA9E5BB9B6BD3A955197FE13F33F7DDA7ECC08E79E0
SHA-512:	7DA2B02627A36C8199814C250A1FBD61A9C18E098F8D691C11D75044E7F51DBD52C31EC2E1EA8CDEE5077ADCCB8CD247266F191292DB661FE7EA1B613FC6468
Malicious:	false

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\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):	298
Entropy (8bit):	4.943030742860529
Encrypted:	false
SSDEEP:	6:zx3M1tFAbQtU1R30qyMstwYVoRRZBXVN+J0fFdCsq2UTiMdH8stCal+n:zK13l30ZMt9BFN+QdCT2UftCM+
MD5:	6A9888952541A41F033EB114C24DC902
SHA1:	41903D7C8F31013C44572E09D97B9AAFBBCE77E6
SHA-256:	41A61D0084CD7884BEA1DF02ED9213CB8C83F4034F5C8156FC5B06D6A3E133CE
SHA-512:	E6AC898E67B4052375FDDFE9894B26D504A7827917BF3E02772CFF45C3FA7CC5E0EFFDC701D208E0DB89F05E42F195B1EC890F316BEE5CB8239AB45444DAA6 E
Malicious:	false
Preview:	Microsoft (R) Build Engine version 4.7.3056.0..[Microsoft .NET Framework, version 4.0.30319.42000]..Copyright (C) Microsoft Corporation. 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 (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.908581539026972
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Order List.exe
File size:	1167872
MD5:	e2893188b7e7d6f19581a7981c2a0a75
SHA1:	6a7a3d1ecb2175b53fb98974220f15ec6a1545cf
SHA256:	09b6f40cf52bde38b03cbf49a02e40370914aacfe727cda9d6d9002cce5debeb
SHA512:	e970d0693a37412f3dc0564298768c9aa105d44b5bc5017f280a7fd3a525181af06d0404f1ded2aabf10f85b6d6812fb189323fabbfde27ba8cc63a3b787449f
SSDEEP:	12288:hMLiJXfXUy8jmk63yoPSaEwvguKt+lCNkogRbHa1U/Fnmb68bEtFqTNmqUQzBRMo:iiwSClPuKtQoWbHWl/024TN+QzrMpnm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0.....>..... .....@.. ....@.....

File Icon

Icon Hash:	e8ccd8d898ac84b0

Static PE Info

General

Entrypoint:	0x4db1ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui

General

Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6107AA90 [Mon Aug 2 08:19:28 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xd91d4	0xd9200	False	0.722661872121	data	7.42920521019	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xdc000	0x43b90	0x43c00	False	0.06349818381	data	3.71639937012	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x120000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/02/21-10:37:48.444296	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	21180	192.168.2.5	79.134.225.115

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Order List.exe PID: 5776 Parent PID: 5704

General

Start time:	10:36:59
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\Order List.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order List.exe'
Imagebase:	0xe50000
File size:	1167872 bytes
MD5 hash:	E2893188B7E7D6F19581A7981C2A0A75
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.319940301.0000000004211000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.319940301.0000000004211000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.319940301.0000000004211000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.320367563.000000000426A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.320367563.000000000426A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.320367563.000000000426A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 1848 Parent PID: 5776

General

Start time:	10:37:40
Start date:	02/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\AylDGlu' /XML 'C:\Users\user\AppData\Local\Temp\tmp5BCE.tmp'
Imagebase:	0x920000
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: 4472 Parent PID: 1848

General

Start time:	10:37:40
Start date:	02/08/2021
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: 5564 Parent PID: 5776

General

Start time:	10:37:41
Start date:	02/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x50000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: MSBuild.exe PID: 4988 Parent PID: 5776

General

Start time:	10:37:42
Start date:	02/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x8d0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
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: 00000012.00000002.504687984.0000000006E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504687984.0000000006E10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504506508.0000000006D90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504506508.0000000006D90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.500969666.0000000003FD6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.493600525.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.493600525.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.493600525.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504550437.0000000006DB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504550437.0000000006DB0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.500557956.0000000003D5E000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504188143.00000000065B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504188143.00000000065B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504614903.0000000006DE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504614903.0000000006DE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504566226.0000000006DC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504566226.0000000006DC0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.503662031.0000000006240000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.503662031.0000000006240000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.503662031.0000000006240000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.503067769.0000000005510000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.503067769.0000000005510000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504637714.0000000006DF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504637714.0000000006DF0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504719426.0000000006E20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504719426.0000000006E20000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504589888.0000000006DD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504589888.0000000006DD0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.496659781.0000000002D01000.00000004.00000001.sdmp, Author: Joe Security

	• Rule: NanoCore, Description: unknown, Source: 00000012.00000002.496659781.0000000002D01000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.496725291.0000000002D80000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.500995543.0000000003FEF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504402260.0000000006D50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504402260.0000000006D50000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504820469.0000000006E60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504820469.0000000006E60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.504524423.0000000006DA0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000012.00000002.504524423.0000000006DA0000.00000004.00000001.sdmp, Author: Florian Roth
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: 3100 Parent PID: 4988

General

Start time:	10:37:44
Start date:	02/08/2021
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\tmp6DFE.tmp'
Imagebase:	0x920000
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: 4692 Parent PID: 3100

General

Start time:	10:37:44
Start date:	02/08/2021
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: schtasks.exe PID: 5512 Parent PID: 4988

General

Start time:	10:37:45
Start date:	02/08/2021
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\tmp71A9.tmp'
Imagebase:	0x920000
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: 1716 Parent PID: 5512

General

Start time:	10:37:45
Start date:	02/08/2021
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

Analysis Process: MSBuild.exe PID: 488 Parent PID: 904

General

Start time:	10:37:45
Start date:	02/08/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe 0
Imagebase:	0xcb0000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 1012 Parent PID: 488

General

Start time:	10:37:46
Start date:	02/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff604460000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5276 Parent PID: 904

General

Start time:	10:37:48
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' 0
Imagebase:	0xa10000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 5284 Parent PID: 5276

General

Start time:	10:37:49
Start date:	02/08/2021
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

Analysis Process: dhcpmon.exe PID: 6080 Parent PID: 3472

General

Start time:	10:37:57
Start date:	02/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xd60000
File size:	261728 bytes
MD5 hash:	D621FD77BD585874F9686D3A76462EF1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 3980 Parent PID: 6080

General

Start time:	10:37:58
Start date:	02/08/2021
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

Disassembly

Code Analysis