ID: 560229
Sample Name: Order Sheet.exe
Cookbook: default.jbs
Time: 09:35:16
Date: 26/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

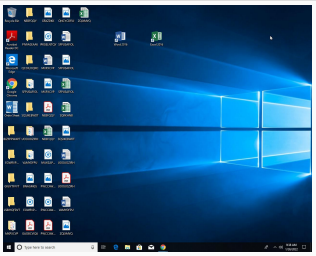
Windows Analysis Report

Order Sheet.exe

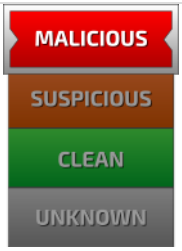
Overview

General Information

Sample Name:	Order Sheet.exe
Analysis ID:	560229
MD5:	8aa38313a97d72.
SHA1:	fa8b4c59dcd2f22..
SHA256:	8d1d485136c3e1..
Tags:	exe NanoCore RAT
Infos:	



Detection



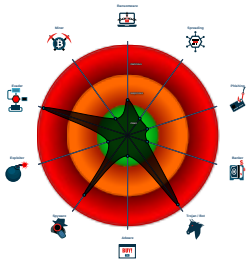
Nanocore AgentTesla

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

Signatures

- Icon mismatch, binary includes an i…
- Yara detected AgentTesla
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for dropped file
- Yara detected Nanocore RAT
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Tries to steal Mail credentials (via fi…
- Initial sample is a PE file and has a…

Classification



Process Tree

- **System is w10x64**
- Order Sheet.exe (PID: 5588 cmdline: "C:\Users\user\Desktop\Order Sheet.exe" MD5: 8AA38313A97D72B6D14B4D067F125086)
  - powershell.exe (PID: 6228 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\Order Sheet.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4088 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2220 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4128 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nXyTfXBfrv" /XML "C:\Users\user\AppData\Local\Temp\tmp87D8.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4100 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Order Sheet.exe (PID: 6200 cmdline: C:\Users\user\Desktop\Order Sheet.exe MD5: 8AA38313A97D72B6D14B4D067F125086)
    - host process.exe (PID: 6076 cmdline: "C:\Users\user\AppData\Local\Temp\host process.exe" 0 MD5: 042FA6CD64D8F55F1405D130E306E47A)
    - O.stub.exe (PID: 6148 cmdline: "C:\Users\user\AppData\Local\Temp\O.stub.exe" 0 MD5: 69709CD1D2019B22E72550ABE3AEF9D7)
- dhcpmon.exe (PID: 2280 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 042FA6CD64D8F55F1405D130E306E47A)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\O.stub.exe	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Users\user\AppData\Local\Temp\host process.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Users\user\AppData\Local\Temp\host process.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
Click to see the 4 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
0000000F.00000000.785845413.0000000000702000.00000002.00000001.01000000.00000005.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000F.00000000.785845413.0000000000702000.00000002.00000001.01000000.00000005.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000F.00000000.785845413.0000000000702000.00000002.00000001.01000000.00000005.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000D.00000003.788250788.0000000003556000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000D.00000003.788376076.000000000106F000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 75 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
15.2.host process.exe.5270000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
15.2.host process.exe.5270000.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
15.0.host process.exe.700000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
15.0.host process.exe.700000.0.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
15.0.host process.exe.700000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 173 entries				

Sigma Overview

AV Detection

Sigma detected: NanoCore

E-Banking Fraud

Sigma detected: NanoCore

System Summary

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Stealing of Sensitive Information

Sigma detected: NanoCore

Remote Access Functionality

Sigma detected: NanoCore

Jbx Signature Overview

AV Detection

Antivirus detection for dropped file

Yara detected Nanocore RAT

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

Uses dynamic DNS services

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Found evasive API chain (trying to detect sleep duration tampering with parallel thread)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected AgentTesla

Yara detected Nanocore RAT

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

Remote Access Functionality

Yara detected AgentTesla

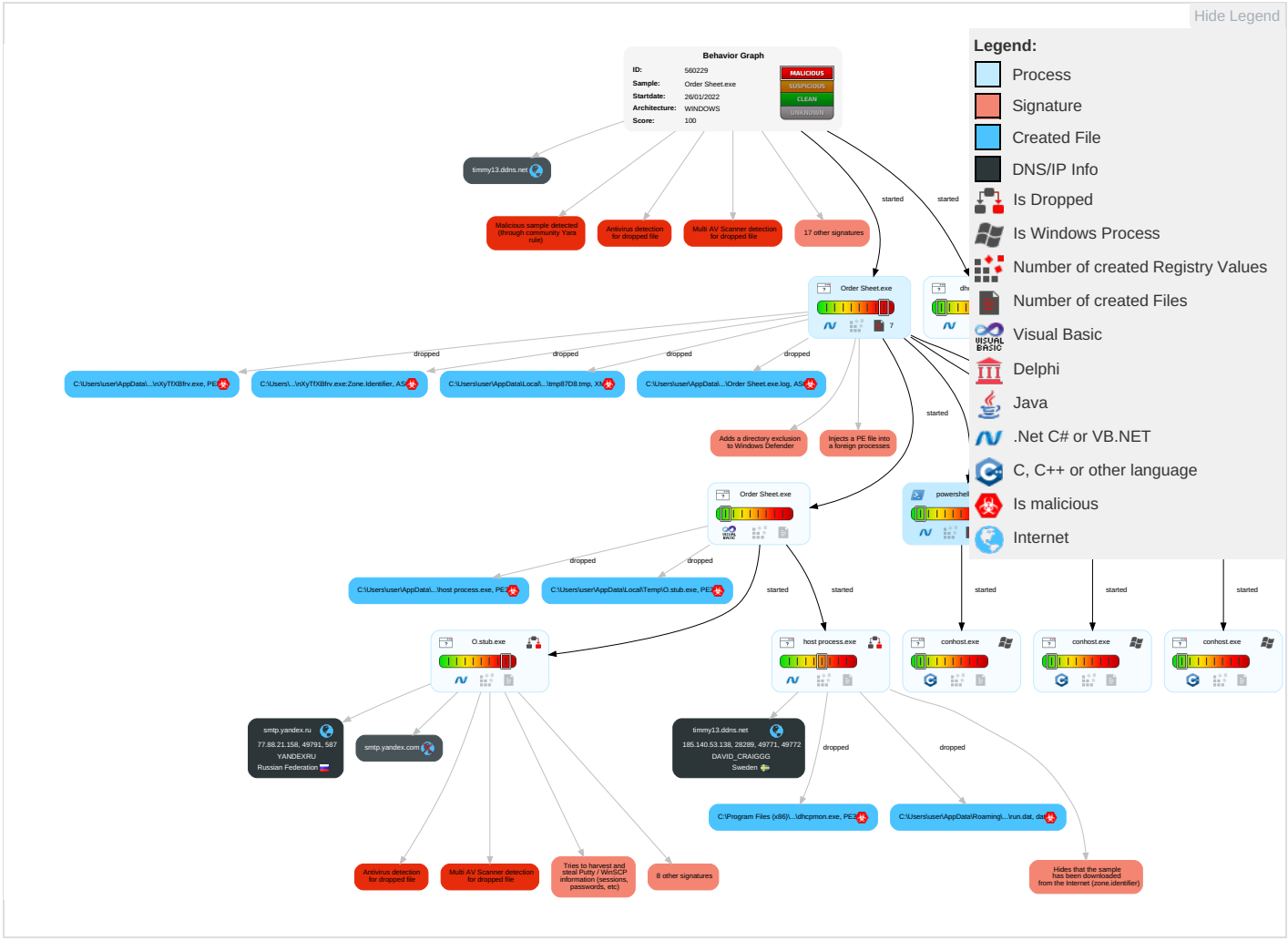
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 1 1 Windows Management Instrumentation	1 Scheduled Task/Job	1 Access Token Manipulation	2 1 Disable or Modify Tools	2 OS Credential Dumping	1 File and Directory Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	1 2 1 Input Capture	1 1 5 System Information Discovery	Remote Desktop Protocol	2 Data from Local System	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Scheduled Task/Job	Logon Script (Windows)	1 Scheduled Task/Job	2 Obfuscated Files or Information	1 Credentials in Registry	1 Query Registry	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 4 Software Packing	NTDS	3 1 1 Security Software Discovery	Distributed Component Object Model	1 2 1 Input Capture	Scheduled Transfer	1 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 2 Masquerading	LSA Secrets	2 Process Discovery	SSH	Keylogging	Data Transfer Size Limits	1 1 1 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 3 1 Virtualization/Sandbox Evasion	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Access Token Manipulation	DCSync	1 Application Window Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 1 2 Process Injection	Proc Filesystem	1 Remote System Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Hidden Files and Directories	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

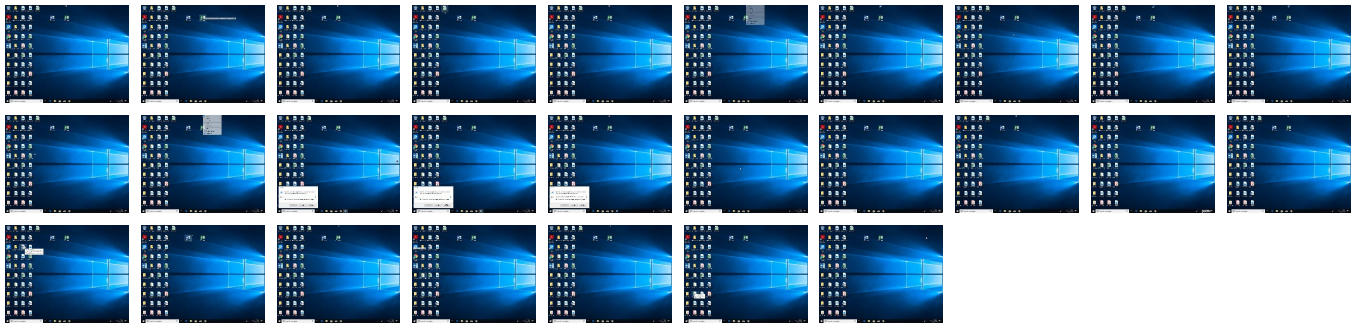
Behavior Graph



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
Order Sheet.exe	25%	Virustotal		Browse
Order Sheet.exe	19%	ReversingLabs	Win32.Trojan.Woreflint	
Order Sheet.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\host process.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Local\Temp\O.stub.exe	100%	Avira	TR/Spy.Gen8	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Local\Temp\host process.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\O.stub.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Local\Temp\O.stub.exe	56%	Metadefender		Browse

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\O.stub.exe	86%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Local\Temp\host process.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe	19%	ReversingLabs	Win32.Trojan.Wordflint	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.2.dhcpmon.exe.6f0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.Order Sheet.exe.400000.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.0.host process.exe.700000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
0.2.Order Sheet.exe.3d59930.4.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.0.O.stub.exe.a10000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
13.0.Order Sheet.exe.400000.12.unpack	100%	Avira	TR/Dropper.Gen		Download File
13.0.Order Sheet.exe.400000.8.unpack	100%	Avira	TR/Dropper.Gen		Download File
16.0.O.stub.exe.a10000.3.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
13.2.Order Sheet.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
17.0.dhcpmon.exe.6f0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.O.stub.exe.a10000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
16.2.O.stub.exe.a10000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
15.0.host process.exe.700000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.Order Sheet.exe.400000.6.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.0.host process.exe.700000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.host process.exe.700000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
16.0.O.stub.exe.a10000.2.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
0.2.Order Sheet.exe.43a1810.7.unpack	100%	Avira	TR/Dropper.Gen		Download File
15.0.host process.exe.700000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
15.2.host process.exe.5620000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	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	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comdiaa	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://https://EZoeItrV4lpBHNUc3pDH.com	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.coma%	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

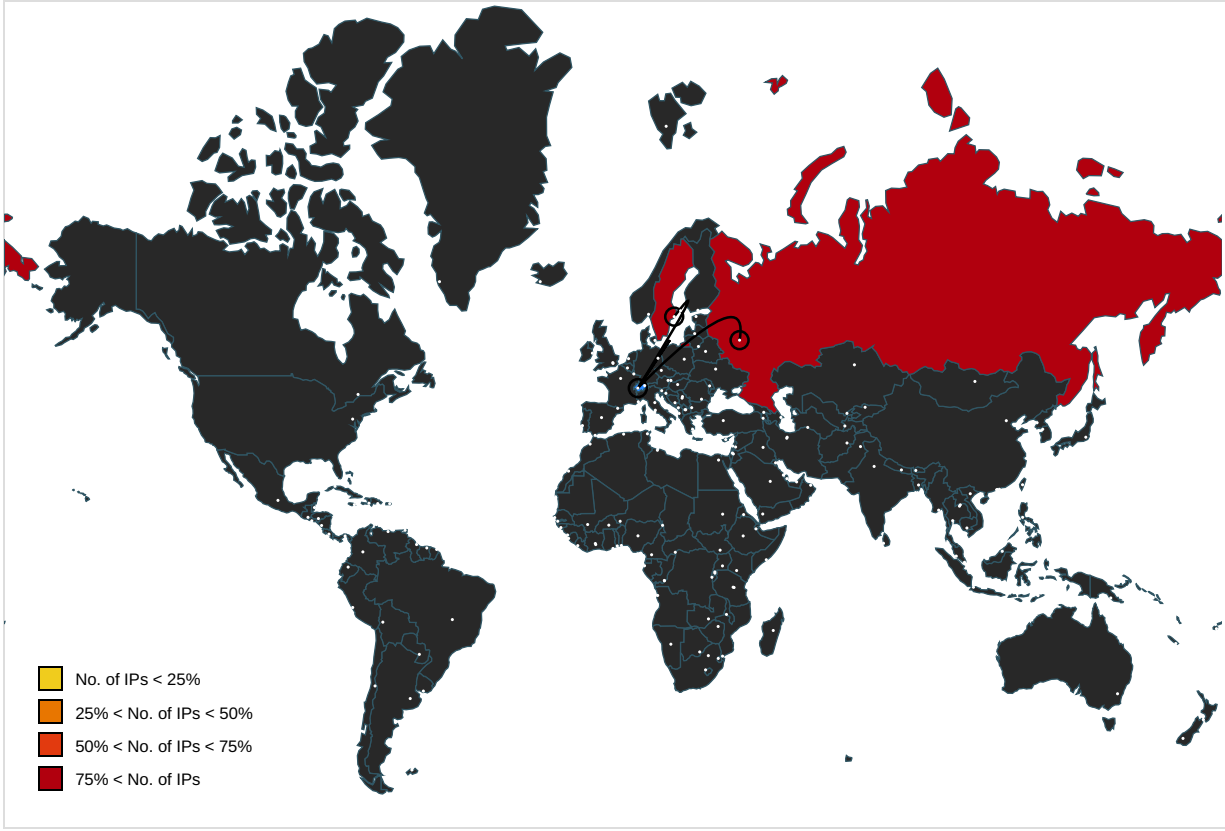
Name	IP	Active	Malicious	Antivirus Detection	Reputation
timmy13.ddns.net	185.140.53.138	true	false		high
smtp.yandex.ru	77.88.21.158	true	false		high
smtp.yandex.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com	Order Sheet.exe, 00000000.00000002.78388 3940.0000000000F67000.00000004.00000020. 00020000.00000000.sdmp, Order Sheet.exe, 00000000.00000002.790648459.0000000006E 12000.00000004.00000800.00020000.0000000 0.sdmp	false		high
http://www.fontbureau.com/designersG	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.tiro.com	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.come.com	Order Sheet.exe, 00000000.00000002.78388 3940.0000000000F67000.00000004.00000020. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.galapagosdesign.com/staff/dennis.htm	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fontbureau.comdiaa	Order Sheet.exe, 00000000.00000002.78388 3940.0000000000F67000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.fonts.com	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://EZoeItrV4lpBHNUc3pDH.com	O.stub.exe, 00000010.00000002.940885541. 0000000003261000.00000004.00000800.00020 000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.zhongyicts.com.cn	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Order Sheet.exe, 00000000.00000002.78466 9508.0000000002D51000.00000004.00000800. 00020000.00000000.sdmp	false		high
http://www.sakkal.com	Order Sheet.exe, 00000000.00000002.79064 8459.0000000006E12000.00000004.00000800. 00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.coma%	Order Sheet.exe, 00000000.00000002.78388 3940.0000000000F67000.00000004.00000020. 00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
77.88.21.158	smtp.yandex.ru	Russian Federation		13238	YANDEXRU	false
185.140.53.138	timmy13.ddns.net	Sweden		209623	DAVID_CRAIGGG	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	560229
Start date:	26.01.2022
Start time:	09:35:16
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order Sheet.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:	25
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.spyw.evad.winEXE@17/16@12/2
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 5.2% (good quality ratio 3.4%) • Quality average: 32.9% • Quality standard deviation: 28.9%
HCA Information:	• Successful, ratio: 94% • 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

- Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, store-images.s-microsoft.com, s-ring.msedge.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, teams-ring.msedge.net, arc.msn.com, t-ring.msedge.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
09:36:36	API Interceptor	2x Sleep call for process: Order Sheet.exe modified
09:36:58	API Interceptor	73x Sleep call for process: powershell.exe modified
09:37:14	API Interceptor	446x Sleep call for process: host process.exe modified
09:37:15	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
09:37:31	API Interceptor	371x Sleep call for process: O.stub.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\host process.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.448972782235035
Encrypted:	false
SSDEEP:	3072:gzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIXquGTziui+IOIB3089u1L5WUb:gLV6Bta6dtJmakIM5jNilOIW8uxb
MD5:	042FA6CD64D8F55F1405D130E306E47A
SHA1:	C7D7DE4600FEB4953D05674F862D992B03E7F44B
SHA-256:	5932288E5C5EF8EDA3E5B63D7E0734123E533FEDCF861A72822004C549606F52
SHA-512:	E5ADD4BB755E59A9244605352612125B026CFAE84118F315594D960359A4795F973A5D9D5B4769FA0A57B607EE075367BA11D209CC6985E931EDDAF531343283
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....- (&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0 ..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly \NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_3 2\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.Vi sualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order Sheet.exe.log	
Process:	C:\Users\user\Desktop\Order Sheet.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	**true**
Reputation:	unknown

Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22300
Entropy (8bit):	5.60227512635438
Encrypted:	false
SSDEEP:	384:ltCDRC0c4BJWXMy909bKc9S0nAjultlub7Y9gBSJ3x6T1MavZlbAV7wWlS5ZBDlj:e0XMMYjTAClth7BcACufw8Vg
MD5:	130FDD38F809F9338F805DAEA9B62136
SHA1:	33A580DDA1B7C67D9D977E8D2C2CE60A57FC6591
SHA-256:	3AA43720B131CDDD1687DEF19222D774CA1442B2D248DF94630A86114C09D8C4
SHA-512:	BBC3AD9526E6F603A15D07E444EB3C0357185E28EE19389F636012EC043691BCEB8BE5D8A3D31777CF1C5FD0775148C93431A20E70B62A47E94ACB8B364E35C0
Malicious:	false
Reputation:	unknown
Preview:	@...e.....h.....X...l.....@.....H.....<@.^.L."My...:U..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...]....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\O.stub.exe

Process:	C:\Users\user\Desktop\Order Sheet.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	283136
Entropy (8bit):	6.583518106694022
Encrypted:	false
SSDEEP:	3072:48lUfsVrpgVIRckQkPIQBoczsDnW+xtUpYslLR8o5s9ODfa8CKeZp/YUNRnoFd18:48lZgPlhKYc2K+p/YUk1wP6D
MD5:	69709CD1D2019B22E72550ABE3AEF9D7
SHA1:	D82D111D5ECB7E2D4DA56C40E9B6EFB409C90243
SHA-256:	B1C71A6054350653138D7C6D9E501DC09E79BCDFD5FECD4F29461B7CA7DA23A4
SHA-512:	5268D185A569FC35CE5761B47713A9D94018A9EA7C9C42EE5942A13722C8D460C3D7760996F21604AA188C24C17EA64DF516D261A73E2BCE5FD75FCBABF8386
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\O.stub.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 56%, Browse • Antivirus: ReversingLabs, Detection: 86%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...Ul.^.....J.....i... .....@.. .....@.....i..W..... ....H.....text....I... ...J..... ..`.rsrc... .....L.....@..@.reloc.....P.....@..B.....i.....H.....L.....q;.SfQ.k..g.2&.0..W.a..JaAN'nG.2N.. .....e..@N.J.....@...DG9.....j...GSENaO.p..u..2..q4.....7...U...]..].h7C2..H.{4.o0:.W.c...C.II*.3Mr.....W.&F~5...J.r6IG{X..X.d..P..F...0.....8GCU.}.r`...._.a.N..0vDjVG..6.9.3.\. ....8....5_X....`.B;.N....N....S_p..em,Rc.9.4_*5..p..kOPulz-.~..@.....v.#K...c.....p&X..K..> rH.Ra...$l.j4.n.."J.S.:..p6.)w...k.@".c..6..G...Ok.w...4....

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_4scc5o5w.sni.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB

SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_fy3orlzq.rnz.ps1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h3pr0zi5.igp.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_hmamsk4v.xr1.psm1

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA46510A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\host process.exe

Process:	C:\Users\user\Desktop\Order Sheet.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.448972782235035
Encrypted:	false
SSDEEP:	3072:gzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIXquGTziui+IOIB3089u1L5WUb:gLV6Bta6dtJmakIM5jNilOIW8uxb
MD5:	042FA6CD64D8F55F1405D130E306E47A
SHA1:	C7D7DE4600FEB4953D05674F862D992B03E7F44B
SHA-256:	5932288E5C5EF8EDA3E5B63D7E0734123E533FEDCF861A72822004C549606F52
SHA-512:	E5ADD4BB755E59A9244605352612125B026CFAE84118F315594D960359A4795F973A5D9D5B4769FA0A57B607EE075367BA11D209CC6985E931EDDAF531343283
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\host process.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\host process.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\host process.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\host process.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....- (&s8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0 ..$.....~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Temp\tmp87D8.tmp

Process:	C:\Users\user\Desktop\Order Sheet.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1597
Entropy (8bit):	5.1406468949426865
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtaMxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTpv
MD5:	7735E0A0B81A5A63D6EA540BE4025893
SHA1:	3AFF867F90FCA54EA918D66A0D4A617F35597F2E
SHA-256:	D1061050FE9D6747753D2CAF4B7991C1DA87271488A189E121819D157FB991D7
SHA-512:	16164642FD7116206CCB2EEC7BAE42163E643F57B1965D622E2FBE3A216419E8B46ABA715175E44B3C18FD9B9BDE8F3EC8D47B3A5A8E588F9A2410538EA4376F
Malicious:	**true**
Reputation:	unknown
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>true</StartWhenAvailable>. <

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

Process:	C:\Users\user\AppData\Local\Temp\host process.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:3jfF8n:x8
MD5:	EF4BC35F382EFDAAA6AC50BE151D16CC
SHA1:	AF893D3A1979E6A574021A61E097B888FDA5668B
SHA-256:	02853E75E5FEC3B59A9EA592B25D651EF3F4D30078C47BDD703BA8D78DC90CD2
SHA-512:	813DD4E36B876765E75D017D0D17D47C13B8F41FA85B582420FD3D3765658585BC11444671F42B6C516F470986CC43CA3373764D56C618777A6995D2CD1B0E85
Malicious:	**true**
Reputation:	unknown
Preview:	.....H

C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe

Process:	C:\Users\user\Desktop\Order Sheet.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1601024
Entropy (8bit):	7.477755094427583
Encrypted:	false
SSDEEP:	49152:gu2h3XxMPoYfBCaTnOfSepK6NNgeG68Nq9Hr2839Y2YXC8bx7wwI3nwiY4gZcaff:uYzfIEOfSP6NNgeG68Nq9Hr2839Y2YXJ
MD5:	8AA38313A97D72B6D14B4D067F125086
SHA1:	FA8B4C59DCD2F226D3DCA64A4B1C8A656F033BD1
SHA-256:	8D1D485136C3E142C31A382E508ED735AD6E290574FE21F754CDFC7CF61ABC43
SHA-512:	AD553AEF980ECA1D9DE9E8C48D46099A19513CBC33929A097AF9E216D36AF8AAF22EFEA131A6E38B9C70ACCE18EAE74A0C4D6FCBE78F050D2EDCEB78AA9F2916
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 19%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0.....F.... .....@.. ....@.....O..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....I.....@..B.....(.....H.....<...x.....@Q.....0..G.....r...p.....,.r...ps....z...(....(.....r...p.o....(....s....z.*.....-.....0..o.....s.... ..s.....~.....(.....o.....,.(.....o .....*...rW..p..o....(....(!.....,..o".....*..(.....-.....4B.....Za.....0..o.....s#.....o$....s%.....+.....J...r...p(&...o'...&...X....i.....-..o(.....&.r...p(!.....,..o".....*.....GO.....

C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe:Zone.Identifier

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

C:\Users\user\Documents\20220126\PowerShell_transcript.928100.iuunlUjd.20220126093659.txt

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5789
Entropy (8bit):	5.405249128810557
Encrypted:	false
SSDEEP:	96:BZ8jGNRvqDo1ZAlZHjGNRvqDo1ZcesGjZIjGNRvqDo1ZozWWnZo:I
MD5:	54891A9A70C35686277A61A955E6759F
SHA1:	13ADD50266AB1FECDEFF5861FA5CFD0C4B91CB64
SHA-256:	8D015F56AFB64F587B06BD018160FA239459734126D52CFF29083B1286C8C534
SHA-512:	033A3CC3D0C14D5C721461CA3EFCC4724E0270CC05ECEEA528235AFEF9D96A0CA0F088E2DF6007AE304AD2DD6B6E851C0B3B4A48A0505F105267BC1565CDE0F9
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126093700..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe..Process ID: 4088..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20220126093700..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe..**********..Windows PowerShell transcript start..Start time: 20220126094126..Username: computer\user..RunAs User: computer\jone

C:\Users\user\Documents\20220126\PowerShell_transcript.928100.tMbosfeB.20220126093657.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	3494
Entropy (8bit):	5.295443301124513
Encrypted:	false
SSDEEP:	96:BZGjGNnqDo1ZwmZ4jGNnqDo1Z2qKr0cr0cr0drZTS:Y//B
MD5:	E8BDC6EADEA4F31A03A6C99D330ACAF5
SHA1:	63AB78EDD34962187766E7A7DA7EA53D5DC75744
SHA-256:	41966A4C53E960589C73C9E70AA496F1117A8B77260E7D09F75955945F863074
SHA-512:	B5A74BA0A47E83FCEDB962215497DE259443676D5B75ADE43DC6F2FE68688BC674036DF88014A850B8C411C17FD4A6135B6349A69F32A74C92C1CF0A3923972
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20220126093658..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 928100 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Order Sheet.exe..Process ID: 6228..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1.. **********..**********..Command start time: 20220126093658..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Order Sheet.exe..**********..Command start time: 20220126094037..**********..PS>TerminatingError(Add-MpPreference): "A positional parameter cannot be found that

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.477755094427583
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 Sheet.exe
File size:	1601024
MD5:	8aa38313a97d72b6d14b4d067f125086
SHA1:	fa8b4c59dcd2f226d3dca64a4b1c8a656f033bd1
SHA256:	8d1d485136c3e142c31a382e508ed735ad6e290574fe21f754cdfc7cf61abc43
SHA512:	ad553aef980eca1d9de9e8c48d46099a19513cbc33929a097af9e216d36af8aaf22efea131a6e38b9c70acce18eae74a0c4d6fcbe78f050d2edceb78aa9f2916
SSDEEP:	49152:gu2h3XxMPoYfBCaTnOfSepK6NNgeG68Nq9Hr2839Y2YXC8bx7wwl3nwiY4gZcaff:uYzfIEOfSP6NNgeG68Nq9Hr2839Y2YXJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....0.....F.... .....@.. ..... @.....

File Icon

Icon Hash:	4f878a8c8e8e874f

Static PE Info

General

Entrypoint:	0x51e746
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61F0A484 [Wed Jan 26 01:31:48 2022 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

Instruction
jmp dword ptr [00402000h]
mov byte ptr [eax-2C754571h], ch
mov ecx, CFB1EDF5h
jmp far 82EBh : FBB5E4AAh
stc
nop
retf B5C9h
out DCh, eax
mov seg?, word ptr [edi-1F081154h]
retf EA8Eh
retf CE80h
lds ebp, fword ptr [ebp-7B2F3B49h]
xchg eax, ebx
aad F0h
jmp 00007F2794BA2B0Ah
mov ah, 9Dh
int3
scasd
movsd
xchg eax, ebp
mov edx, 9DD28799h
jecxz 00007F2794BA2AD3h
mov edx, 0000CA90h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11e6f4	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x120000	0x6a100	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x18c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x11c78c	0x11c800	False	0.790293071727	data	7.73049016205	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x120000	0x6a100	0x6a200	False	0.217102841578	data	5.70309311156	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x18c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1202e0	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x120748	0x988	data		
RT_ICON	0x1210d0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4294440951, next used block 4294440951		
RT_ICON	0x122178	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4294440951, next used block 4294440951		
RT_ICON	0x124720	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 4294440951, next used block 4294440951		
RT_ICON	0x128948	0x5488	data		
RT_ICON	0x12ddd0	0x94a8	data		
RT_ICON	0x137278	0x10828	data		
RT_ICON	0x147aa0	0x42028	data		
RT_GROUP_ICON	0x189ac8	0x84	data		
RT_GROUP_ICON	0x189b4c	0x14	data		
RT_VERSION	0x189b60	0x3b4	data		
RT_MANIFEST	0x189f14	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2012
Assembly Version	1.5.0.0
InternalName	EnumerateQueuedWorkItemsd.exe
FileVersion	22.0.3.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	iiInfinityEngine Application
ProductVersion	22.0.3.0
FileDescription	iiInfinityEngine Application
OriginalFilename	EnumerateQueuedWorkItemsd.exe

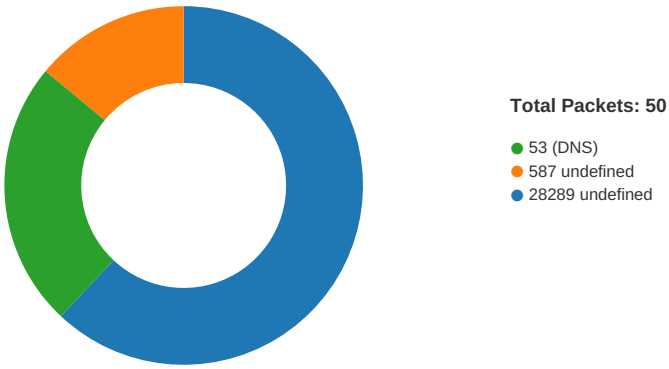
Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-09:37:20.272699	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58028	8.8.8.8	192.168.2.4
01/26/22-09:37:28.793156	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	53097	8.8.8.8	192.168.2.4

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/26/22-09:37:35.309243	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49257	8.8.8.8	192.168.2.4
01/26/22-09:38:00.114032	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56621	8.8.8.8	192.168.2.4
01/26/22-09:38:19.365908	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61721	8.8.8.8	192.168.2.4
01/26/22-09:38:24.484006	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51255	8.8.8.8	192.168.2.4

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 09:37:20.284939051 CET	49771	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:20.309189081 CET	28289	49771	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:20.985627890 CET	49771	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:21.010018110 CET	28289	49771	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:21.595035076 CET	49771	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:21.619411945 CET	28289	49771	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:28.809151888 CET	49772	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:28.835051060 CET	28289	49772	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:29.487339020 CET	49772	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:29.511679888 CET	28289	49772	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:30.095736027 CET	49772	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:30.120399952 CET	28289	49772	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:35.438718081 CET	49775	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:35.463648081 CET	28289	49775	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:36.011564016 CET	49775	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:36.036777020 CET	28289	49775	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:36.721287012 CET	49775	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:36.756702900 CET	28289	49775	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:45.345719099 CET	49782	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:45.369750977 CET	28289	49782	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:45.987684011 CET	49782	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:46.011650085 CET	28289	49782	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:46.597110987 CET	49782	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:46.621114969 CET	28289	49782	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:53.208463907 CET	49785	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:53.232434034 CET	28289	49785	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:53.816437960 CET	49785	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:53.840488911 CET	28289	49785	185.140.53.138	192.168.2.4
Jan 26, 2022 09:37:54.504038095 CET	49785	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:37:54.528040886 CET	28289	49785	185.140.53.138	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 09:37:58.171214104 CET	49791	587	192.168.2.4	77.88.21.158
Jan 26, 2022 09:37:58.240809917 CET	587	49791	77.88.21.158	192.168.2.4
Jan 26, 2022 09:37:58.240943909 CET	49791	587	192.168.2.4	77.88.21.158
Jan 26, 2022 09:37:58.403897047 CET	587	49791	77.88.21.158	192.168.2.4
Jan 26, 2022 09:37:58.404520035 CET	49791	587	192.168.2.4	77.88.21.158
Jan 26, 2022 09:37:58.473668098 CET	587	49791	77.88.21.158	192.168.2.4
Jan 26, 2022 09:37:58.473753929 CET	587	49791	77.88.21.158	192.168.2.4
Jan 26, 2022 09:37:58.474026918 CET	49791	587	192.168.2.4	77.88.21.158
Jan 26, 2022 09:37:58.520803928 CET	49791	587	192.168.2.4	77.88.21.158
Jan 26, 2022 09:37:58.543967009 CET	587	49791	77.88.21.158	192.168.2.4
Jan 26, 2022 09:37:58.544141054 CET	49791	587	192.168.2.4	77.88.21.158
Jan 26, 2022 09:37:58.590092897 CET	587	49791	77.88.21.158	192.168.2.4
Jan 26, 2022 09:37:58.590195894 CET	49791	587	192.168.2.4	77.88.21.158
Jan 26, 2022 09:38:00.120090008 CET	49794	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:00.144737005 CET	28289	49794	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:00.785784006 CET	49794	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:00.810064077 CET	28289	49794	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:01.395205021 CET	49794	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:01.419224977 CET	28289	49794	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:07.200850010 CET	49815	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:07.225295067 CET	28289	49815	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:07.739521027 CET	49815	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:07.765228033 CET	28289	49815	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:08.270811081 CET	49815	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:08.295097113 CET	28289	49815	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:13.381500006 CET	49820	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:13.405689001 CET	28289	49820	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:13.911890030 CET	49820	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:13.936033964 CET	28289	49820	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:14.443311930 CET	49820	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:14.467354059 CET	28289	49820	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:19.369946003 CET	49822	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:19.394294977 CET	28289	49822	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:19.896815062 CET	49822	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:19.921241999 CET	28289	49822	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:20.428132057 CET	49822	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:20.452897072 CET	28289	49822	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:24.488524914 CET	49824	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:24.517618895 CET	28289	49824	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:25.131593943 CET	49824	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:25.155803919 CET	28289	49824	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:25.741022110 CET	49824	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:25.764976025 CET	28289	49824	185.140.53.138	192.168.2.4
Jan 26, 2022 09:38:29.823460102 CET	49825	28289	192.168.2.4	185.140.53.138
Jan 26, 2022 09:38:29.847364902 CET	28289	49825	185.140.53.138	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 09:37:20.251436949 CET	58028	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:37:20.272699118 CET	53	58028	8.8.8.8	192.168.2.4
Jan 26, 2022 09:37:28.772248030 CET	53097	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:37:28.793155909 CET	53	53097	8.8.8.8	192.168.2.4
Jan 26, 2022 09:37:35.287247896 CET	49257	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:37:35.309242964 CET	53	49257	8.8.8.8	192.168.2.4
Jan 26, 2022 09:37:45.305258989 CET	49910	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:37:45.326595068 CET	53	49910	8.8.8.8	192.168.2.4
Jan 26, 2022 09:37:53.186959028 CET	64549	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:37:53.206617117 CET	53	64549	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 26, 2022 09:37:58.129935980 CET	56534	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:37:58.150065899 CET	53	56534	8.8.8.8	192.168.2.4
Jan 26, 2022 09:38:00.092590094 CET	56621	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:38:00.114032030 CET	53	56621	8.8.8.8	192.168.2.4
Jan 26, 2022 09:38:07.134366989 CET	64078	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:38:07.152343035 CET	53	64078	8.8.8.8	192.168.2.4
Jan 26, 2022 09:38:13.343151093 CET	64801	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:38:13.362807989 CET	53	64801	8.8.8.8	192.168.2.4
Jan 26, 2022 09:38:19.346575975 CET	61721	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:38:19.365907907 CET	53	61721	8.8.8.8	192.168.2.4
Jan 26, 2022 09:38:24.461409092 CET	51255	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:38:24.484005928 CET	53	51255	8.8.8.8	192.168.2.4
Jan 26, 2022 09:38:29.803133965 CET	61522	53	192.168.2.4	8.8.8.8
Jan 26, 2022 09:38:29.822896957 CET	53	61522	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 26, 2022 09:37:20.251436949 CET	192.168.2.4	8.8.8.8	0xa9ce	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:28.772248030 CET	192.168.2.4	8.8.8.8	0x55d	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:35.287247896 CET	192.168.2.4	8.8.8.8	0x714d	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:45.305258989 CET	192.168.2.4	8.8.8.8	0xbd6c	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:53.186959028 CET	192.168.2.4	8.8.8.8	0xbc91	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:58.129935980 CET	192.168.2.4	8.8.8.8	0x6b0f	Standard query (0)	smtp.yandex.com	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:00.092590094 CET	192.168.2.4	8.8.8.8	0x3bbb	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:07.134366989 CET	192.168.2.4	8.8.8.8	0x15c8	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:13.343151093 CET	192.168.2.4	8.8.8.8	0xe257	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:19.346575975 CET	192.168.2.4	8.8.8.8	0xfcc7	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:24.461409092 CET	192.168.2.4	8.8.8.8	0x49c	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:29.803133965 CET	192.168.2.4	8.8.8.8	0x3024	Standard query (0)	timmy13.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2022 09:37:20.272699118 CET	8.8.8.8	192.168.2.4	0xa9ce	No error (0)	timmy13.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:28.793155909 CET	8.8.8.8	192.168.2.4	0x55d	No error (0)	timmy13.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:35.309242964 CET	8.8.8.8	192.168.2.4	0x714d	No error (0)	timmy13.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:45.326595068 CET	8.8.8.8	192.168.2.4	0xbd6c	No error (0)	timmy13.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:53.206617117 CET	8.8.8.8	192.168.2.4	0xbc91	No error (0)	timmy13.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:37:58.150065899 CET	8.8.8.8	192.168.2.4	0x6b0f	No error (0)	smtp.yandex.com	smtp.yandex.ru		CNAME (Canonical name)	IN (0x0001)
Jan 26, 2022 09:37:58.150065899 CET	8.8.8.8	192.168.2.4	0x6b0f	No error (0)	smtp.yandex.ru		77.88.21.158	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:00.114032030 CET	8.8.8.8	192.168.2.4	0x3bbb	No error (0)	timmy13.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:07.152343035 CET	8.8.8.8	192.168.2.4	0x15c8	No error (0)	timmy13.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:13.362807989 CET	8.8.8.8	192.168.2.4	0xe257	No error (0)	timmy13.ddns.net		185.140.53.138	A (IP address)	IN (0x0001)

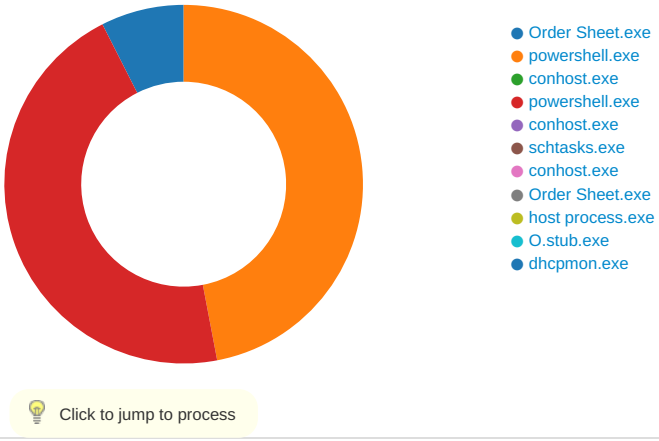
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 26, 2022 09:38:19.365907907 CET	8.8.8.8	192.168.2.4	0xfcc7	No error (0)	timmy13.dd ns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:24.484005928 CET	8.8.8.8	192.168.2.4	0x49c	No error (0)	timmy13.dd ns.net		185.140.53.138	A (IP address)	IN (0x0001)
Jan 26, 2022 09:38:29.822896957 CET	8.8.8.8	192.168.2.4	0x3024	No error (0)	timmy13.dd ns.net		185.140.53.138	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jan 26, 2022 09:37:58.403897047 CET	587	49791	77.88.21.158	192.168.2.4	220 sas2-34ddad429748.qloud-c.yandex.net ESMTP (Want to use Yandex.Mail for your domain? Visit http://pdd.yandex.ru) 1643186278-2XpDuhdd9g-bwHijw0x
Jan 26, 2022 09:37:58.404520035 CET	49791	587	192.168.2.4	77.88.21.158	EHLO 928100
Jan 26, 2022 09:37:58.473753929 CET	587	49791	77.88.21.158	192.168.2.4	250-sas2-34ddad429748.qloud-c.yandex.net 250-8BITMIME 250-PIPELINING 250-SIZE 53477376 250-STARTTLS 250-AUTH LOGIN PLAIN XOAUTH2 250-DSN 250 ENHANCEDSTATUSCODES
Jan 26, 2022 09:37:58.474026918 CET	49791	587	192.168.2.4	77.88.21.158	STARTTLS
Jan 26, 2022 09:37:58.543967009 CET	587	49791	77.88.21.158	192.168.2.4	220 Go ahead

Statistics

Behavior



System Behavior

Analysis Process: Order Sheet.exe PID: **5588**, Parent PID: **6732**

General

Target ID:	0
Start time:	09:36:12
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\Order Sheet.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Order Sheet.exe"
Imagebase:	0x720000
File size:	1601024 bytes

MD5 hash:	8AA38313A97D72B6D14B4D067F125086
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.784669508.0000000002D51000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.785591112.0000000003D59000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.785591112.0000000003D59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.785591112.0000000003D59000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.785591112.0000000003D59000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.786336359.0000000003F23000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.786336359.0000000003F23000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.786336359.0000000003F23000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.786336359.0000000003F23000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E33CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E33CF06	unknown
C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6D18DD66	CopyFileW
C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6D18DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp87D8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6D187038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order Sheet.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E64C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
unknown	success or wait	1	6D186A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 11 00 00 fd 06 00 00 00 00 00 46 fd 11 00 00 20 00 00 00 00 12 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 18 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELa0F @ @	success or wait	7	6D18DD66	CopyFileW
C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6D18DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp87D8.tmp	0	1597	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20	<?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>	success or wait	1	6D181B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Order Sheet.exe.log	0	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E64C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E31CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D181B4F	ReadFile

Analysis Process: powershell.exe PID: **6228**, Parent PID: **5588**

General

Target ID:	7
Start time:	09:36:55
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\Desktop\Order Sheet.exe
Imagebase:	0x7ff732050000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E33CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E33CF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D0E5B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D0E5B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4scc5o5w.sni.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D181E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_h3pr0zi5.igp.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D181E60	CreateFileW
C:\Users\user\Documents\20220126	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6D18BEFF	CreateDirectoryW
C:\Users\user\Documents\20220126\PowerShell_transcript.928100.tMbosfeB.20220126093657.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D181E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4scc5o5w.sni.ps1	success or wait	1	6D186A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_h3pr0zi5.igp.psm1	success or wait	1	6D186A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_4scc5o5w.sni.ps1	0	1	31	1	success or wait	1	6D181B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_h3pr0zi5.igp.psm1	0	1	31	1	success or wait	1	6D181B4F	WriteFile
C:\Users\user\Documents\20220126\PowerShell_transcript.928100.tMbosfeB.20220126093657.txt	0	3	ff		success or wait	1	6D181B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20220126\PowerShell_transcript.928100.tMbosfeB.20220126093657.txt	3	670	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 36 30 39 33 36 35 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 39 32 38 31 30 30 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220126093658Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 928100 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	30	6D181B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 7f 14 00 00 19 00 00 00 68 0d fd 04 fd 08 fd 08 fd 08 00 00 fd 00 58 00 08 00 49 0d 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@ehXI@	success or wait	1	6E6076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 55 00 00 00 0e 00 20 00	H<@^L"My:U	success or wait	16	6E6076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	16	6E6076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	10	6E6076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1084	4	54 00 00 02	T	success or wait	10	6E6076FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1088	2044	01 00 00 00 00 00 00 00 01 00 00 00 fd 37 fd 2c fd 66 69 44 fd 17 fd 1a fd 0d fd fd fd 00 00 00 0e 00 2a 00 4d 69 63 72 6f 73 6f 66 74 2e 4d 61 6e 61 67 65 6d 65 6e 74 2e 49 6e 66 72 61 73 74 72 75 63 74 75 72 65 2e 4e 61 74 69 76 65 00 00 00 08 00 03 00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 56 00 40 00 fd 01 40 00 fd 00 40 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40	7,fiD*Microsoft.Management.Infrastructure.NativeV@@@T@>@@V@H@X@[@NT@HT@S@S@hT@g@@@S@S@S@\@T@T@@X@?X@T@S@S@T@T@xT@zT@	success or wait	10	6E6076FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E31CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E31CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E31CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E315705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E321F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6E32203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2703DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	7	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	11	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	6E2FD72F	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6E2FD72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	6E2FD72F	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D181B4F	ReadFile

Analysis Process: conhost.exe PID: **6220**, Parent PID: **6228**

General

Target ID:	8
Start time:	09:36:56
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: powershell.exe PID: **4088**, Parent PID: **5588**

General

Target ID:	9
Start time:	09:36:57
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\nXyTfXBfrv.exe
Imagebase:	0x1d0000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E33CF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6E33CF06	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fy3orlzq.rnz.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D181E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hmamsk4v.xr1.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6D181E60	CreateFileW
C:\Users\user\Documents\20220126\PowerShell_transcript.928100.iuunIUjd.20220126093659.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6D181E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fy3orlzq.rnz.ps1	success or wait	1	6D186A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hmamsk4v.xr1.psm1	success or wait	1	6D186A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_fy3orlzq.rnz.ps1	0	1	31	1	success or wait	1	6D181B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_hmamsk4v.xr1.psm1	0	1	31	1	success or wait	1	6D181B4F	WriteFile
C:\Users\user\Documents\20220126\PowerShell_transcript.928100.iuunIUjd.20220126093659.txt	0	3	ff		success or wait	1	6D181B4F	WriteFile
C:\Users\user\Documents\20220126\PowerShell_transcript.928100.iuunIUjd.20220126093659.txt	3	677	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 32 30 31 32 36 30 39 33 37 30 30 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 39 32 38 31 30 30 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 43 3a 5c 57 69	**********Windows PowerShell transcript startStart time: 20220126093700Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 928100 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6D181B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	0	64	40 00 00 01 65 00 00 00 00 00 00 00 11 00 00 00 7f 14 00 00 19 00 00 00 68 0d fd 04 fd 08 fd 08 fd 08 00 00 fd 00 58 00 08 00 49 0d 00 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00	@ehXI@	success or wait	1	6E6076FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	64	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 fd 5e 7f 4c fd 22 4d 79 fd fd fd 3a 55 00 00 00 0e 00 20 00	H<@^L"My:U	success or wait	17	6E6076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	104	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	17	6E6076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E6076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6E6076FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1172	2044	00 0e fd 00 01 0e fd 00 02 0e fd 00 03 0e fd 00 04 0e fd 00 05 0e fd 00 06 0e fd 00 07 0e fd 00 08 0e fd 00 09 0c fd 00 56 00 40 00 fd 01 40 00 fd 00 40 00 54 01 40 00 fd 3e 40 01 fd 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 fd 53 40 01 fd 53 40 01 68 54 40 01 fd 67 40 01 fd 01 40 00 fd 00 40 00 fd 53 40 01 fd 53 40 01 fd 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 fd 53 40 01 fd 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 fd 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 fd 44 40 01 fd 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 16 3b 40 01 1b 3b 40 01 19 3b 40 01 fd 3c 40 01 fd 3c 40 01 fd 3c 40	V@@@T@>@@V@H@X@[@NT@HT@S@S@hT@ g@@@S@S@S@\@T@T@@X@? X@T@S@S@T@ T@xT@zT@T@=M@DM@:M@"M@ M@!M@;M @D@D@@M@<M@$M@8M@? M@;@;@;@<@<@<@	success or wait	11	6E6076FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E31CA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E31CA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E31CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E315705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E321F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23192	success or wait	1	6E32203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2703DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	143	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6D181B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D181B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2703DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2703DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E315705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6D181B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	73	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	11	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	13	6D181B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6D181B4F	ReadFile

Analysis Process: conhost.exe PID: **2220**, Parent PID: **4088**

General

Target ID:	10
Start time:	09:36:57
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: **4128**, Parent PID: **5588**

General

Target ID:	11
Start time:	09:36:58
Start date:	26/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\nXyTfXBfrv" /XML "C:\Users\user\AppData\Local\Temp\tmp87D8.tmp
Imagebase:	0xc60000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **4100**, Parent PID: **4128**

General

Target ID:	12
Start time:	09:36:59
Start date:	26/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
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: Order Sheet.exe PID: **6200**, Parent PID: **5588**

General

Target ID:	13
Start time:	09:37:01
Start date:	26/01/2022
Path:	C:\Users\user\Desktop\Order Sheet.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Order Sheet.exe
Imagebase:	0x710000
File size:	1601024 bytes
MD5 hash:	8AA38313A97D72B6D14B4D067F125086
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000003.788250788.0000000003556000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000003.788376076.000000000106F000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.778355649.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.778355649.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.778355649.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.778355649.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.777156532.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000000.777156532.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.777156532.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.777156532.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.794132877.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000D.00000002.794132877.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.794132877.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.794132877.0000000000403000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000003.791041172.00000000034F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: host process.exe PID: **6076**, Parent PID: **6200**

General

Target ID:	15
Start time:	09:37:08
Start date:	26/01/2022

Path:	C:\Users\user\AppData\Local\Temp\host process.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\host process.exe" 0
Imagebase:	0x700000
File size:	207360 bytes
MD5 hash:	042FA6CD64D8F55F1405D130E306E47A
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: 0000000F.00000000.785845413.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.785845413.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.785845413.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.786290846.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.786290846.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.786290846.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.785282794.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.785282794.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.785282794.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.941244676.0000000003E89000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.941244676.0000000003E89000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.942025681.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.942025681.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.942025681.0000000005620000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.934558154.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.934558154.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.934558154.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.941790490.0000000005270000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000F.00000002.941790490.0000000005270000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000000.786907867.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000000.786907867.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000000.786907867.0000000000702000.00000002.00000001.01000000.00000005.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\host process.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\host process.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\host process.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\host process.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 100%, ReversingLabs
Reputation:	low

Analysis Process: O.stub.exe PID: **6148**, Parent PID: **6200**

General

Target ID:	16
Start time:	09:37:10
Start date:	26/01/2022
Path:	C:\Users\user\AppData\Local\Temp\O.stub.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Local\Temp\O.stub.exe" 0
Imagebase:	0xa10000
File size:	283136 bytes
MD5 hash:	69709CD1D2019B22E72550ABE3AEF9D7

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.790298908.0000000000A12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.934638725.0000000000A12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.789340353.0000000000A12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.790790305.0000000000A12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000002.940720707.000000000315C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000010.00000002.940720707.000000000315C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000010.00000000.789744754.0000000000A12000.00000002.00000001.01000000.00000006.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: C:\Users\user\AppData\Local\Temp\O.stub.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 56%, Metadefender, Browse • Detection: 86%, ReversingLabs
Reputation:	low

Analysis Process: dhcpmon.exe PID: **2280**, Parent PID: **3424**

General

Target ID:	17
Start time:	09:37:24
Start date:	26/01/2022
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x6f0000
File size:	207360 bytes
MD5 hash:	042FA6CD64D8F55F1405D130E306E47A
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: 00000011.00000000.819202402.00000000006F2000.00000002.00000001.01000000.00000007.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000000.819202402.00000000006F2000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000000.819202402.00000000006F2000.00000002.00000001.01000000.00000007.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.839950628.0000000003E11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.839950628.0000000003E11000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.839877068.0000000002E11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.839877068.0000000002E11000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000011.00000002.839063926.00000000006F2000.00000002.00000001.01000000.00000007.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.839063926.00000000006F2000.00000002.00000001.01000000.00000007.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.839063926.00000000006F2000.00000002.00000001.01000000.00000007.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 100%, ReversingLabs
Reputation:	low

Disassembly

No disassembly