ID: 561384
Sample Name: HOANG HA TRADING - PRODUCTS LIST.exe
Cookbook: default.jbs
Time: 12:43:18
Date: 27/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

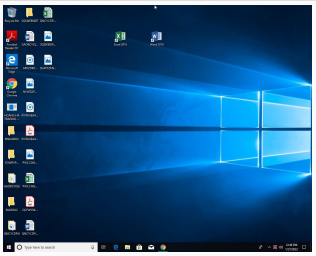
Windows Analysis Report

HOANG HA TRADING - PRODUCTS LIST.exe

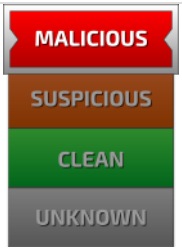
Overview

General Information

Sample Name:	HOANG HA TRADING - PRODUCTS LIST.exe
Analysis ID:	561384
MD5:	3588f04ddba594..
SHA1:	1b350c789c3882..
SHA256:	f35f5f2a4c1f89f2..
Tags:	exe NanoCore RAT
Infos:	



Detection



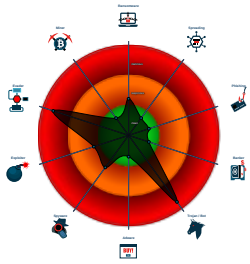
Nanocore

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Antivirus detection for URL or domain
- Multi AV Scanner detection for drop…
- Yara detected Nanocore RAT
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…

Classification



Process Tree

- **System is w10x64**
- HOANG HA TRADING - PRODUCTS LIST.exe (PID: 3576 cmdline: "C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe" MD5: 3588F04DDBA594909215FFA819D1A655)
  - powershell.exe (PID: 6284 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\XWhIIIO.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6292 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6300 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\XWhIIIO" /XML "C:\Users\user\AppData\Local\Temp\tmpF354.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6400 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - HOANG HA TRADING - PRODUCTS LIST.exe (PID: 6440 cmdline: C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe MD5: 3588F04DDBA594909215FFA819D1A655)
  - HOANG HA TRADING - PRODUCTS LIST.exe (PID: 6460 cmdline: C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe MD5: 3588F04DDBA594909215FFA819D1A655)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "2df65f40-d688-48d5-8802-f573ead9",
  "Group": "BILLION-1",
  "Domain1": "62.197.136.188",
  "Domain2": "127.0.0.1",
  "Port": 4052,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.553479253.0000000006850000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2205:$x1: NanoCore.ClientPluginHost • 0x223e:$x2: IClientNetworkHost
0000000D.00000002.553479253.0000000006850000.00000004.08000000.00040000.00000000.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2205:$x2: NanoCore.ClientPluginHost • 0x2320:$s4: PipeCreated • 0x221f:$s5: IClientLoggingHost
0000000D.00000000.338178828.0000000000402000.00000040.00000400.00020000.00000000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000D.00000000.338178828.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000D.00000000.338178828.0000000000402000.00000040.00000400.00020000.00000000.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

Click to see the 57 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
13.2.HOANG HA TRADING - PRODUCTS LIST.exe.3b3aa04.13.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1deb:$x1: NanoCore.ClientPluginHost • 0x1e24:$x2: IClientNetworkHost

Source	Rule	Description	Author	Strings
13.2.HOANG HA TRADING - PRODUCTS LIST.exe.3b3aa04.13.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x1deb:$x2: NanoCore.ClientPluginHost • 0x1f36:$s4: PipeCreated • 0x1e05:$s5: IClientLoggingHost
13.2.HOANG HA TRADING - PRODUCTS LIST.exe.6870000.27.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x3deb:$x1: NanoCore.ClientPluginHost • 0x3f48:$x2: IClientNetworkHost
13.2.HOANG HA TRADING - PRODUCTS LIST.exe.6870000.27.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x3deb:$x2: NanoCore.ClientPluginHost • 0x4d41:$s3: PipeExists • 0x3fe1:$s4: PipeCreated • 0x3e05:$s5: IClientLoggingHost
13.0.HOANG HA TRADING - PRODUCTS LIST.exe.400000.12.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 144 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

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Nanocore RAT

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

Boot Survival

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

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected Nanocore RAT

Remote Access Functionality

Detected Nanocore Rat

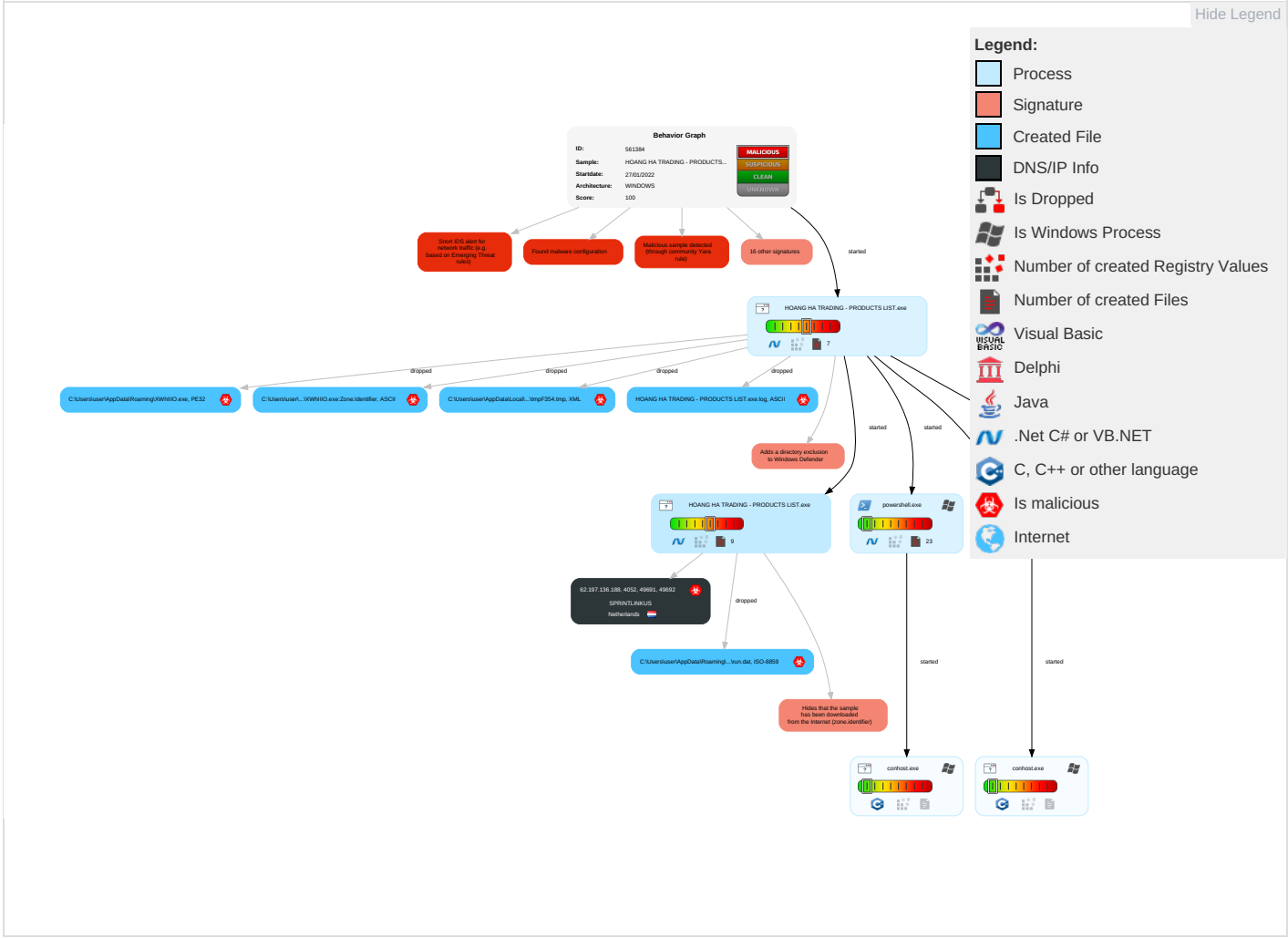
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Windows Management Instrumentation	1 Scheduled Task/Job	1 2 Process Injection	1 Masquerading	1 1 Input Capture	1 System Time Discovery	Remote Services	1 1 Input Capture	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 1 1 Security Software Discovery	Remote Desktop Protocol	1 1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 1 Virtualization/Sandbox Evasion	Security Account Manager	2 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 Remote Access Software	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 2 Process Injection	NTDS	2 1 Virtualization/Sandbox Evasion	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Deobfuscate/Decode Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Hidden Files and Directories	Cached Domain Credentials	1 File and Directory Discovery	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	3 Obfuscated Files or Information	DCSync	1 3 System Information 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 3 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

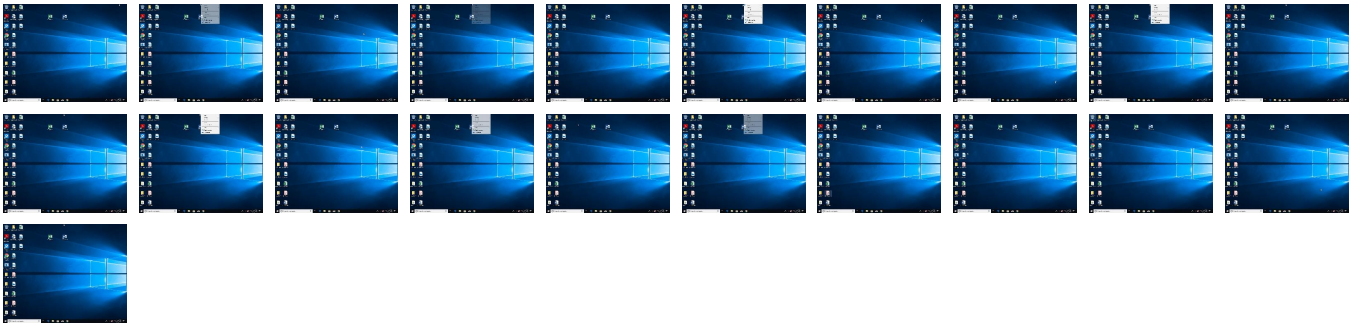
Behavior Graph



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
HOANG HA TRADING - PRODUCTS LIST.exe	39%	Virustotal		Browse
HOANG HA TRADING - PRODUCTS LIST.exe	42%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
HOANG HA TRADING - PRODUCTS LIST.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\XWhIIIO.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\XWhIIIO.exe	39%	Virustotal		Browse
C:\Users\user\AppData\Roaming\XWhIIIO.exe	42%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.HOANG HA TRADING - PRODUCTS LIST.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.HOANG HA TRADING - PRODUCTS LIST.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.HOANG HA TRADING - PRODUCTS LIST.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.HOANG HA TRADING - PRODUCTS LIST.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.0.HOANG HA TRADING - PRODUCTS LIST.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
13.2.HOANG HA TRADING - PRODUCTS LIST.exe.5ba0000.19.unpack	100%	Avira	TR/NanoCore.fadte		Download File
13.0.HOANG HA TRADING - PRODUCTS LIST.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		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.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.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
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://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
62.197.136.188	0%	Virustotal		Browse
62.197.136.188	100%	Avira URL Cloud	malware	
127.0.0.1	0%	Virustotal		Browse
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

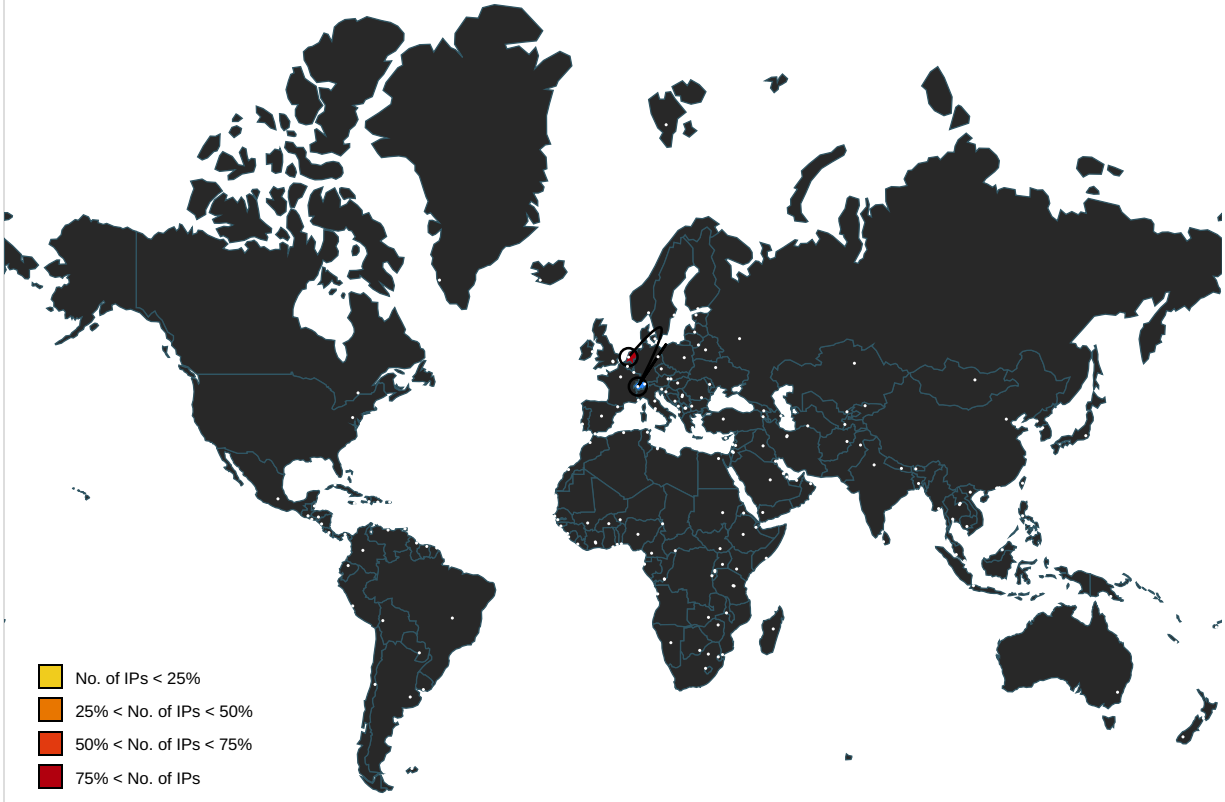
Name	Malicious	Antivirus Detection	Reputation
62.197.136.188	true	• 0%, Virustotal, Browse • Avira URL Cloud: malware	unknown
127.0.0.1	true	• 0%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.apache.org/licenses/LICENSE-2.0	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designersG	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers/?	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.tiro.com	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.goodfont.co.kr	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://google.com	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000D.00000002.551380125.0000000003C5F000.00000004.00000800.00020000.00000000.sdmp, HOANG HA TRADING - PRODUCTS LIST.exe, 0000000D.00000002.553508914.0000000006870000.00000004.08000000.00040000.00000000.sdmp, HOANG HA TRADING - PRODUCTS LIST.exe, 0000000D.00000002.548918331.00000000029DB000.00000004.00000800.00020000.00000000.sdmp, HOANG HA TRADING - PRODUCTS LIST.exe, 0000000D.00000002.550917756.0000000003B35000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sajatypeworks.com	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/cThe	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/frere-jones.html	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers8	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fonts.com	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.urwpp.deDPlease	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.341610591.0000000003071000.00000004.00000800.00020000.00000000.sdmp, HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.341051623.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, HOANG HA TRADING - PRODUCTS LIST.exe, 0000000D.00000002.548853139.0000000002971000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sakkal.com	HOANG HA TRADING - PRODUCTS LIST.exe, 00000000.00000002.345205902.0000000006EF2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
62.197.136.188	unknown	Netherlands		1239	SPRINTLINKUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	561384
Start date:	27.01.2022
Start time:	12:43:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 36s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	HOANG HA TRADING - PRODUCTS LIST.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@11/12@0/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 0.7% (good quality ratio 0.2%) • Quality average: 29.6% • Quality standard deviation: 40.7%
HCA Information:	• Successful, ratio: 99% • 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

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Execution Graph export aborted for target HOANG HA TRADING - PRODUCTS LIST.exe, PID 6440 because there are no executed function
- Not all processes where analyzed, report is missing behavior 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
12:44:25	API Interceptor	771x Sleep call for process: HOANG HA TRADING - PRODUCTS LIST.exe modified
12:44:34	API Interceptor	43x Sleep call for process: powershell.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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HOANG HA TRADING - PRODUCTS LIST.exe.log

Process:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.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:	high, very likely benign file
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):	22392
Entropy (8bit):	5.602882216687213
Encrypted:	false
SSDEEP:	384:vtCDTTuvS9LB/U3iUS0nwjultIq77Y9gxSJ3xuT1MavZlbAV7hG5ZBDI+Rzg:6L5VUTwCltlfxcECmfwwVU
MD5:	9C89704256AD8C57C919C8F3A1917F1F
SHA1:	C522CEAB4DF358A608BB2A76C22AFA9D27EEC6B2
SHA-256:	6B121252553C385EF891E89523310000B4E1EBF87664C3A4FFFF640A59D9A23D
SHA-512:	03A10C03655897BF0BC77F50400D2D378ED6D6CC4930F12102D07C8696889AD52C71F288BC464FE3054BDC77FCEE56CD195EB6EDF909EF30D8507D38763B782

Malicious:	false
Reputation:	low
Preview:	@...e.....h._.....H.....@.....H.....<@.^.L."My...:U..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.....Sy stem.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__PSScriptPolicyTest_bqbado0i.lol.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_s1oslob1.c5k.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:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 0A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpF354.tmp

Process:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1594
Entropy (8bit):	5.147636160167977
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtT5xvn:cge4MYrFdOFzOzN33ODOiDdKrsuTTvv
MD5:	3467A7468FBE38A32CCD7F661AE64948
SHA1:	3B5EC15B81BDD0B6C6F68263A4BD7B9C9630FFEA
SHA-256:	195C8447F05F5552179030C801AC2C5FB6DFDC8850A721EF809A541B5E77BF06
SHA-512:	FF61B32AFE5A40300CA709A603AF8397C31AF57DE832486C3AF20226CBB0827ACFC61DAF81BCF9772D91B53AF1FBBE374EC6CED2133EB116E2B0C63101A3F7 6D
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-1 0-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserI d>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Princip al id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <Sto pIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35A5
Malicious:	false
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
File Type:	ISO-8859 text, with CR line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:RVt:ft
MD5:	BAE6600FA534ABB76FA969A360070C58
SHA1:	3186B5081965D71EECFE535DD37309A2D031583E
SHA-256:	5F2F02A0DE97B689C732B6B71CB72D7F66FA6CF63FC97BB80E9722D23CACCDE5
SHA-512:	BED83063E01450FC57C3A4825AE872AA2EC3714DF66E0162806CF181B16314F580807EB482D236D3324E857EB4D6AD2019C923EF271D1D925E26305F0B52759D
Malicious:	**true**
Preview:	[.....H

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
File Type:	data
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85

SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E926
Malicious:	false
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.I.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h.._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r.....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. I..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

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

Process:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	441856
Entropy (8bit):	7.834985196744199
Encrypted:	false
SSDEEP:	6144:qpMFO+Q45IX8LhyTamQH7mDiZX0YIH9gCAMcKb/beI8mAWilDJC0qTs1EoHMHK/5:SXFH9gdMcMN8pJK3WMq/UOtL0eZ
MD5:	3588F04DDBA594909215FFA819D1A655
SHA1:	1B350C789C3882ACAC391806DBC1ECB44632A297
SHA-256:	F35F5F2A4C1F89F26553DDB83C8DF510A492873975224DEE57E386B9FBC0795A
SHA-512:	2AAE9F314D6A7ACD4C6607FEED54B0EA31331E5D7BD1D77C7B2F70B29646BF17CA0717C159E53548378F88289D5179188B7635C9B4E0504FD391B9206F56E45
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 39%, Browse • Antivirus: ReversingLabs, Detection: 42%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....".a.....0.....b.... .....@.. ....@.....O..... ....H.....text...h.... ....`.rsrc.....@..@.reloc..... .....@..B.....D.....H.....xD.. .....Z.....@.....(.....}.....{....{....s...}.....(.....*..0.....{.....+..*&...}....*...0.....+,...+...{..... (.....X...{.....-....X...{.....-..{.....{.....[.Y.{.....[.Y.X(.....{.....{.....[.Y.{.....[.O(.....{.....{.....[.{.....[.Y.O(.....{.....{.....[.{.....[.X(....*..0.....s....}.....(.....(.....{.....o.....(.....{.....o..... (.....{.....o.....(.....{.....o.....(

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

Process:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20220127\PowerShell_transcript.284992.tH6b1Aws.20220127124433.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):	5777
Entropy (8bit):	5.4161494278237505
Encrypted:	false
SSDEEP:	96:BZ8hUNtqDo1ZvZHhUNtqDo1Z8F3tjZchUNtqDo1ZRQddSZF:/
MD5:	7C45F52AC1D0360FD0C66DC7621109C6
SHA1:	AC35EF33601A39DB921BBB1D3A9D3C6E3A7974BD
SHA-256:	E4FC8EACB1E2AC6693B72B658CC0C5D59D8F2A2F5D6D64E8FB53769C84966D7F
SHA-512:	89A16298E90A6C7C57756483735104BDD45FDC2708A00D35D9B04741DE88620DD310CEDA7EA846D36177FAE2BA46B1C9EDFF1805665182E305386E57A384F1B
Malicious:	false

Preview:	.**********..Windows PowerShell transcript start..Start time: 20220127124434..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 284992 (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\XWhIIIO.exe..Process ID: 6284..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: 20220127124434..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\XWhIIIO.exe..**********..Windows PowerShell transcript start..Start time: 20220127124837..Username: computer\user..RunAs User: computer\user..Con

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.834985196744199
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:	HOANG HA TRADING - PRODUCTS LIST.exe
File size:	441856
MD5:	3588f04ddba594909215ffa819d1a655
SHA1:	1b350c789c3882acac391806dbc1ecb44632a297
SHA256:	f35f5f2a4c1f89f26553ddb83c8df510a492873975224dee57e386b9fbc0795a
SHA512:	2aae9f314d6a7acd4c6607feed54b0ea31331e5d7bd1d77c7b2f70b29646bf17ca0717c159e53548378f88289d5179188b7635c9b4e0504fd391b9206f56e45e
SSDEEP:	6144:qpMFO+Q45IX8LhyTamQH7mDiZX0YIH9gCAMcKb/beI8mAWilDJC0qTs1EoHMHK/5:SXFH9gdMcMN8pJK3WMq/UOtL0eZ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...".a.....0.....b.... ....@.. .... @.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x46d362
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:	0x61F2228A [Thu Jan 27 04:41:46 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]
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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x6d310	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6e000	0x5f8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x70000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x6d1d8	0x1c	.text
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	0x6b368	0x6b400	False	0.905489692599	data	7.84240410344	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x6e000	0x5f8	0x600	False	0.4296875	data	4.20859981737	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x70000	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_VERSION	0x6e090	0x366	data		
RT_MANIFEST	0x6e408	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 Overwolf 2021
Assembly Version	11.0.0.0
InternalName	HashElementEnt.exe
FileVersion	11.0.0.0
CompanyName	Overwolf LTD
LegalTrademarks	
Comments	
ProductName	Overwolf
ProductVersion	11.0.0.0
FileDescription	Overwolf
OriginalFilename	HashElementEnt.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/22-12:44:46.390279	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49691	4052	192.168.2.3	62.197.136.188
01/27/22-12:44:52.932033	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49692	4052	192.168.2.3	62.197.136.188
01/27/22-12:44:59.456999	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49694	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:07.015474	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49695	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:13.058509	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49696	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:19.802384	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49697	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:25.746771	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:31.854870	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49699	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:37.809917	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49700	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:43.827723	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49701	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:48.874690	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49702	4052	192.168.2.3	62.197.136.188
01/27/22-12:45:53.922190	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49703	4052	192.168.2.3	62.197.136.188

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/27/22-12:45:59.081946	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49704	4052	192.168.2.3	62.197.136.188
01/27/22-12:46:05.073938	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	4052	192.168.2.3	62.197.136.188
01/27/22-12:46:11.147135	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49706	4052	192.168.2.3	62.197.136.188
01/27/22-12:46:15.825425	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49707	4052	192.168.2.3	62.197.136.188

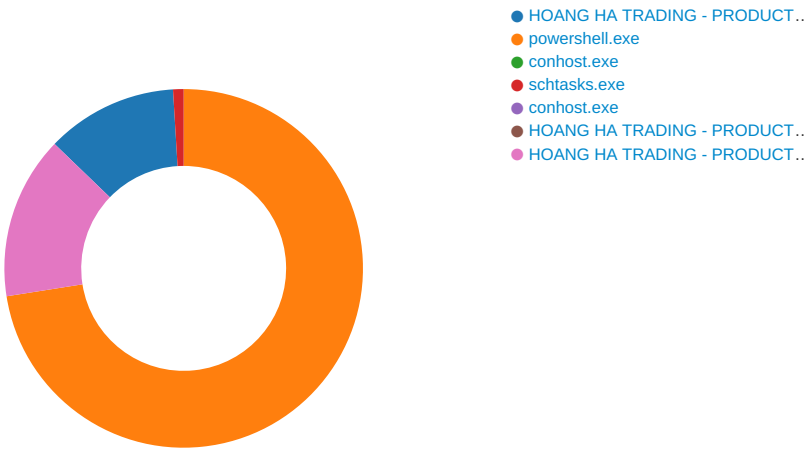
TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 12:44:46.214098930 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:46.241147995 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:46.241326094 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:46.390279055 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:46.431857109 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:46.480118036 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:46.514540911 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:46.655117989 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:46.677963018 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:46.730134964 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.019212008 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.156794071 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.156900883 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.176754951 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.176815033 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.176856995 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.176879883 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.176894903 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.176923990 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.176932096 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.176954031 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.204154968 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.204216957 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.204261065 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.204301119 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.204317093 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.204338074 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.204377890 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.204380989 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.204417944 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.204451084 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.204458952 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.204524040 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.231389046 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231450081 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231487989 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231527090 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231535912 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.231565952 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231605053 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.231606007 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231647015 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231684923 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231689930 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.231724024 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231756926 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.231765032 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231803894 CET	4052	49691	62.197.136.188	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 27, 2022 12:44:47.231838942 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.231844902 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231884956 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231916904 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.231924057 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231965065 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.231990099 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.232003927 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.232069016 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259080887 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259139061 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259180069 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259234905 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259273052 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259311914 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259341955 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259356976 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259397984 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259402037 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259408951 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259438038 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259464025 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259475946 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259515047 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259532928 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259555101 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259593010 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259630919 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259633064 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259668112 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259704113 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259707928 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259751081 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259772062 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259788990 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259829044 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259851933 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259869099 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259907007 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259941101 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.259947062 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.259985924 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.260009050 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.260025024 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.260066032 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.260087967 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.260102034 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.260143042 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.260164976 CET	49691	4052	192.168.2.3	62.197.136.188
Jan 27, 2022 12:44:47.260180950 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.260221004 CET	4052	49691	62.197.136.188	192.168.2.3
Jan 27, 2022 12:44:47.260251045 CET	49691	4052	192.168.2.3	62.197.136.188

Statistics

Behavior



System Behavior

Analysis Process: HOANG HA TRADING - PRODUCTS LIST.exe PID: **3576**, Parent PID: **3408**

General

Target ID:	0
Start time:	12:44:08
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe"
Imagebase:	0xa60000
File size:	441856 bytes
MD5 hash:	3588F04DDBA594909215FFA819D1A655
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.343719392.0000000003F19000.00000004.00000800.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.343719392.0000000003F19000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.343719392.0000000003F19000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.341610591.0000000003071000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.341051623.0000000002F11000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
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	6E3CCF06	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	6E3CCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\XWhIIIO.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	6C40DD66	CopyFileW
C:\Users\user\AppData\Roaming\XWhIIIO.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C40DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpF354.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C407038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HOANG HA TRADING - PRODUCTS LIST.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E6DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF354.tmp	success or wait	1	6C406A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\XWhIIIO.exe	0	131072	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 22 fd 61 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 fd 06 00 00 08 00 00 00 00 00 00 62 fd 06 00 00 20 00 00 00 fd 06 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 20 07 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.$PEL"a0b @ @	success or wait	4	6C40DD66	CopyFileW
C:\Users\user\AppData\Roaming\XWhIIIO.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	6C40DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF354.tmp	0	1594	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 68 61 72 64 7a 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	6C401B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\HOANG HA TRADING - PRODUCTS LIST.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	6E6DC907	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	6E3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3A5705	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C401B4F	ReadFile

Analysis Process: powershell.exe PID: **6284**, Parent PID: **3576**

General

Target ID:	8
Start time:	12:44:32
Start date:	27/01/2022
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\XWhIIIO.exe
Imagebase:	0xac0000
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	6E3CCF06	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	6E3CCF06	unknown
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_s1oslob1.c5k.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_bqbado0i.lol.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW
C:\Users\user\Documents\20220127	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C40BEFF	CreateDirectoryW
C:\Users\user\Documents\20220127\PowerShell_transcript.284992.tH6b1Aws.20220127124433.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_s1oslob1.c5k.ps1	success or wait	1	6C406A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PScriptPolicyTest_bqbado0i.lol.psm1	success or wait	1	6C406A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_s1oslob1.c5k.ps1	0	1	31	1	success or wait	1	6C401B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_bqbado0i.lol.psm1	0	1	31	1	success or wait	1	6C401B4F	WriteFile
C:\Users\user\Documents\20220127\PowerShell_transcript.284992.tH6b1Aws.20220127124433.txt	0	3	ff		success or wait	1	6C401B4F	WriteFile
C:\Users\user\Documents\20220127\PowerShell_transcript.284992.tH6b1Aws.20220127124433.txt	3	674	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 37 31 32 34 34 33 34 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 68 61 72 64 7a 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 68 61 72 64 7a 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 32 38 34 39 39 32 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: 20220127124434Username: computer\userRunAs User: computer\userConfiguration Name: Machine: 284992 (Microsoft Windows NT 10.0.17134.0)Host Application: C:\Wi	success or wait	44	6C401B4F	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 fd 14 00 00 1b 00 00 00 68 0d 5f 04 08 09 fd 08 fd 08 00 00 fd 00 fd 00 0c 00 48 0d 00 00 00 00 00 00 00 00 04 40 00 fd 00 00 00 00 00 00 00 00	@eh_H@	success or wait	1	6E6976FC	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	17	6E6976FC	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	6E6976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	255	1	00		success or wait	11	6E6976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	1168	4	00 08 00 03		success or wait	11	6E6976FC	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
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 54 01 40 00 fd 3e 40 01 56 00 40 00 fd 01 40 00 fd 00 40 00 fd 00 40 00 fd 67 40 01 fd 01 40 00 fd 00 40 00 07 0c fd 00 56 01 40 00 07 0e fd 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 53 40 01 fd 53 40 01 08 0c fd 00 fd 53 40 01 08 0e fd 00 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 12 6f 40 01 2a 29 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 1f 29 40 01 4d 64 40 01 5d 64 40 01 20 4d 40 01 4e 64 40 01 21 4d 40 01 fd 29 40 01 fd 29 40 01 23 29 40 01 5c 64 40 01 5a 64 40 01 5b 64 40 01 3b 4d 40	T@>@V@@@@g@@ @V@H@X@[@NT@HT @S@S @hT@S@S@S@\@T@ T@@X@? X@T@S@S@o@ *)@T@T@xT@zT@T@ =M@DM@:M@"M@)@ Md@]d@ M@Nd@!M@)@)@#)@\ d@Zd@[d@;M@	success or wait	11	6E6976FC	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	6E3A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E3ACA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E3ACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E3A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E3A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E3A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	6E3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3A5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	6E3B1F73	ReadFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	23196	success or wait	1	6E3B203F	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3003DE	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	6C401B4F	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	6C401B4F	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	6C401B4F	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	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	124	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	6C401B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppBackgroundTask\AppBackgroundTask.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppLocker\AppLocker.psd1	unknown	990	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AppvClient\AppvClient.psd1	unknown	4096	end of file	1	6C401B4F	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	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E3A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E3A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Appx\Appx.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\AssignedAccess\AssignedAccess.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	8	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	6E3A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	6E3A5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psd1	unknown	368	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	4096	success or wait	3	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\en-US\BitLocker.psd1	unknown	770	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	success or wait	60	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	104	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitLocker\BitLocker.psm1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	522	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BitsTransfer\BitsTransfer.psd1	unknown	4096	end of file	1	6C401B4F	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	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	358	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\BranchCache\BranchCache.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	160	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\CimCmdlets\CimCmdlets.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	699	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\Defender.psd1	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpComputerStatus.cdxml	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	success or wait	10	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	764	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpPreference.cdxml	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	617	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreat.cdxml	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatCatalog.cdxml	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpThreatDetection.cdxml	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	227	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpScan.cdxml	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	243	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpSignature.cdxml	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Defender\MSFT_MpWDOScan.cdxml	unknown	4096	end of file	1	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	4096	success or wait	2	6C401B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psd1	unknown	637	end of file	2	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	4096	success or wait	16	6C401B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft.PowerShell.Utility.psm1	unknown	128	end of file	2	6C401B4F	ReadFile

Analysis Process: conhost.exe PID: **6292**, Parent PID: **6284**

General

Target ID:	9
Start time:	12:44:32
Start date:	27/01/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: **6300**, Parent PID: **3576**

General

Target ID:	10
Start time:	12:44:32
Start date:	27/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\XWhIIIO" /XML "C:\Users\user\AppData\Local\Temp\tmpF354.tmp
Imagebase:	0x1020000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpF354.tmp	unknown	2	success or wait	1	102AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpF354.tmp	unknown	1595	success or wait	1	102ABD9	ReadFile

Analysis Process: conhost.exe PID: **6400**, Parent PID: **6300**

General

Target ID:	11
Start time:	12:44:33
Start date:	27/01/2022

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: HOANG HA TRADING - PRODUCTS LIST.exe PID: **6440**, Parent PID: **3576**

General

Target ID:	12
Start time:	12:44:34
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
Imagebase:	0x350000
File size:	441856 bytes
MD5 hash:	3588F04DDBA594909215FFA819D1A655
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: HOANG HA TRADING - PRODUCTS LIST.exe PID: **6460**, Parent PID: **3576**

General

Target ID:	13
Start time:	12:44:35
Start date:	27/01/2022
Path:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe
Imagebase:	0x490000
File size:	441856 bytes
MD5 hash:	3588F04DDBA594909215FFA819D1A655
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: 0000000D.00000002.553479253.0000000006850000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553479253.0000000006850000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.338178828.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.338178828.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.338178828.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.548853139.0000000002971000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553495828.0000000006860000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553495828.0000000006860000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.551380125.0000000003C5F000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553508914.0000000006870000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source:

	0000000D.00000002.553508914.0000000006870000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553295380.00000000066E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553295380.00000000066E0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.338501190.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.338501190.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.338501190.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.552629896.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.552629896.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.552629896.0000000005BA0000.00000004.08000000.00040000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.550429661.00000000039D0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.552875368.0000000005F50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.552875368.0000000005F50000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553457385.0000000006840000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553457385.0000000006840000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.552454196.00000000051B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.552454196.00000000051B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553587766.00000000068B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553587766.00000000068B0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553547292.0000000006890000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553547292.0000000006890000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553529227.0000000006880000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553529227.0000000006880000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.337767531.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.337767531.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.337767531.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553655349.0000000006900000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553655349.0000000006900000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.547124757.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.547124757.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.547124757.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000000.338846811.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000000.338846811.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000000.338846811.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553237518.0000000006570000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553237518.0000000006570000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000D.00000002.553603368.00000000068C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 0000000D.00000002.553603368.00000000068C0000.00000004.08000000.00040000.00000000.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.548918331.00000000029DB000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.550917756.0000000003B35000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.550917756.0000000003B35000.00000004.00000800.00020000.00000000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6E3CCF06	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	6E3CCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C40BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C40BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C40BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	12	6C401E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C401E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe:Zone.Identifier	success or wait	1	6C382935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	0	8	5b 0d fd fd fd fd fd 48	[H	success or wait	1	6C401B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	0	232	47 6a fd 68 5c fd 33 fa 41 fd fd fd 35 fd 78 fd fd 26 15 fd fd 69 2b fd 49 63 28 31 fd 50 fd fd 50 fd 63 4c 54 fd fd 42 41 fd 62 fd fd 1b fd fd fd fd fd 34 68 fd 12 fd 74 fd 2b fd 07 5a 5c fd fd 20 fd 69 fd fd a4 fd fd 40 fd 33 fd fd 7b 0c fd 1c 67 72 76 2b 56 fd fd fd 42 19 0e fd 0d fd fd 15 5d fd 50 fd fd 16 57 fd 34 43 7d 75 4c 1e fd fd 0b fd 73 7e fd fd 46 04 fd fd 7d fd fd fd fd fd 00 45 fd fd fd fd fd fd 45 fd 14 fd 36 45 fd fd fd fd fd 7b 5f 05 18 7b fd 79 53 fd fd fd 37 fd fd 22 16 68 4b fd 21 03 78 fd 32 fd fd 69 e3 fd 7a 4a fd bb fd 20 fd fd fd fd 66 fd 67 3f fd 5f 0b fd fd fd 30 fd 3a 65 5b 37 77 7b 31 fd 21 fd 34 fd fd fd fd fd 26 fd	Gjh\3A5x&i+c(1PPcLTAb 4ht+Z\ i@ 3{grv+VB]PW4C}uLs~F} EE6E{{yS7"hK!x2izJ f? _0:e[7w{1!4&	success or wait	9	6C401B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	0	327432	70 54 eb fd 21 fd 08 57 fd fd 47 14 4a fd fd 61 60 29 17 40 8b 69 fd fd 77 70 4b fd 73 6f 40 fd 06 fd 35 fd 3d 10 5e fd 1d 51 fd 6f 79 fd 3d 65 40 39 fd 42 fd fd fd 46 fd fd 30 39 75 22 33 fd fd 20 30 74 fd 19 52 44 6e 5f 34 64 fd fd 17 02 fd 45 fd fd 06 69 fd 08 fd fd fd fd 7e 0c fd fd 7c fd fd 66 58 5f 0e fd fd 58 66 fd 70 5e fd fd fd fd 03 fd 3e 61 cb fd 24 fd fd fd 65 05 36 3a 37 64 fd 28 61 05 41 fd fd fd 3d fd 29 2a 0d fd fd fd fd 7b 42 1c 5b fd fd fd 79 25 fd 2a 31 fd 69 fd 51 fd 3c 12 90 78 74 29 58 13 11 48 09 fd 20 fd 24 48 46 37 67 0f fd fd 49 fd 2a 33 03 7b 0c 6e fd fd fd fd 4c 5b 79 3b 69 fd fd 73 2d 1e fd fd fd 28 35 69 8b fd fd 10 fd fd 02 fd fd 08 17 4a 09 35 62 37 7d fd fd 66 4b fd fd 48 56	pT!WGJa)@iwpKso@5=^ Qoy=e@9BF09u"3 0tRDn_4dEi~|fX_Xfp^>a$ e6:7d(aA=)* {B[y%*iQ<xtXH HF7gI*3{nLy;is- (5iJ5b7}fKHV	success or wait	1	6C401B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	0	40	39 69 48 fd 1a c5 7d 5a cd 34 00 fd 66 0d 7e 61 fd fd fd 01 06 fd 0c fd 7e fd 7e fd fd fd fd 05 fd fd 33 fd 55 0b	9iH}Z4f~a~~3U	success or wait	1	6C401B4F	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	6E3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E3003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E3003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C401B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C401B4F	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe	unknown	4096	success or wait	1	6E38D72F	unknown
C:\Users\user\Desktop\HOANG HA TRADING - PRODUCTS LIST.exe	unknown	512	success or wait	1	6E38D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6E38D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E38D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6E38D72F	unknown

Disassembly

No disassembly