ID: 527594
Sample Name: Purchase Order.exe
Cookbook: default.jbs
Time: 01:47:08
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

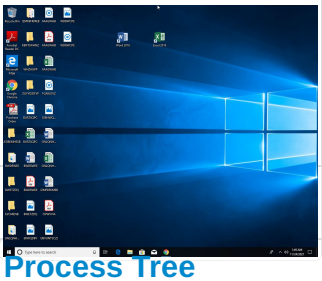
Windows Analysis Report Purchase Order.exe

Overview

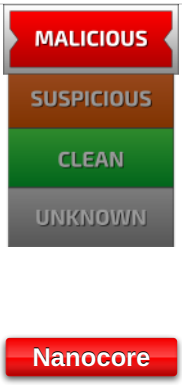
General Information

Sample Name:	Purchase Order.exe
Analysis ID:	527594
MD5:	c7ac272d4cfd98c..
SHA1:	a6334818159cc0..
SHA256:	443c27b78b0fa24.
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection

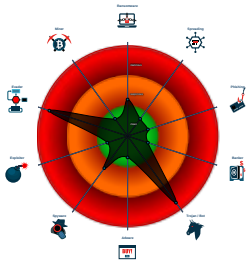


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Snort IDS alert for network traffic (e....
- Malicious sample detected (through ...
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp...
- Yara detected Nanocore RAT
- Initial sample is a PE file and has a ...
- Tries to detect sandboxes and other...
- Sigma detected: Suspicius Add Tas...
- .NET source code contains potentia...
- Injects a PE file into a foreign proce...

Classification



Process Tree

- **System is w10x64**
- Purchase Order.exe (PID: 6284 cmdline: "C:\Users\user\Desktop\Purchase Order.exe" MD5: C7AC272D4CFD98C9D86BFF3B6C3E89D8)
  - powershell.exe (PID: 4544 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\HxuauFbNyB.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6792 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6816 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HxuauFbNyB" /XML "C:\Users\user\AppData\Local\Temp\tmp4FFB.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5664 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase Order.exe (PID: 3416 cmdline: C:\Users\user\Desktop\Purchase Order.exe MD5: C7AC272D4CFD98C9D86BFF3B6C3E89D8)
    - schtasks.exe (PID: 5280 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp65C6.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 7044 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp6E05.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- Purchase Order.exe (PID: 7052 cmdline: "C:\Users\user\Desktop\Purchase Order.exe" 0 MD5: C7AC272D4CFD98C9D86BFF3B6C3E89D8)
  - powershell.exe (PID: 5684 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\HxuauFbNyB.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5628 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5712 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HxuauFbNyB" /XML "C:\Users\user\AppData\Local\Temp\tmpAF9F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4240 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Purchase Order.exe (PID: 5600 cmdline: C:\Users\user\Desktop\Purchase Order.exe MD5: C7AC272D4CFD98C9D86BFF3B6C3E89D8)
- dhcpmon.exe (PID: 1440 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: C7AC272D4CFD98C9D86BFF3B6C3E89D8)
- dhcpmon.exe (PID: 5248 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: C7AC272D4CFD98C9D86BFF3B6C3E89D8)
  - powershell.exe (PID: 4780 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\HxuauFbNyB.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6636 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HxuauFbNyB" /XML "C:\Users\user\AppData\Local\Temp\tmpB24F.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 7072 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 5980 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: C7AC272D4CFD98C9D86BFF3B6C3E89D8)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000016.00000000.714576190.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000016.00000000.714576190.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000016.00000000.714576190.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$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
00000016.00000000.715150890.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000016.00000000.715150890.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 81 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.Purchase Order.exe.3b44c4d.4.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0x24170:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost • 0x2419d:$x2: IClientNetworkHost
22.2.Purchase Order.exe.3b44c4d.4.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xb184:$x2: NanoCore.ClientPluginHost • 0x24170:$x2: NanoCore.ClientPluginHost • 0xc25f:$s4: PipeCreated • 0x2524b:$s4: PipeCreated • 0xb19e:$s5: IClientLoggingHost • 0x2418a:$s5: IClientLoggingHost
22.2.Purchase Order.exe.3b44c4d.4.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
22.2.Purchase Order.exe.3b40624.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x28799:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x287c6:$x2: IClientNetworkHost
22.2.Purchase Order.exe.3b40624.5.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x28799:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x29874:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x287b3:$s5: IClientLoggingHost
Click to see the 111 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

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

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

Uses dynamic DNS services

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

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:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

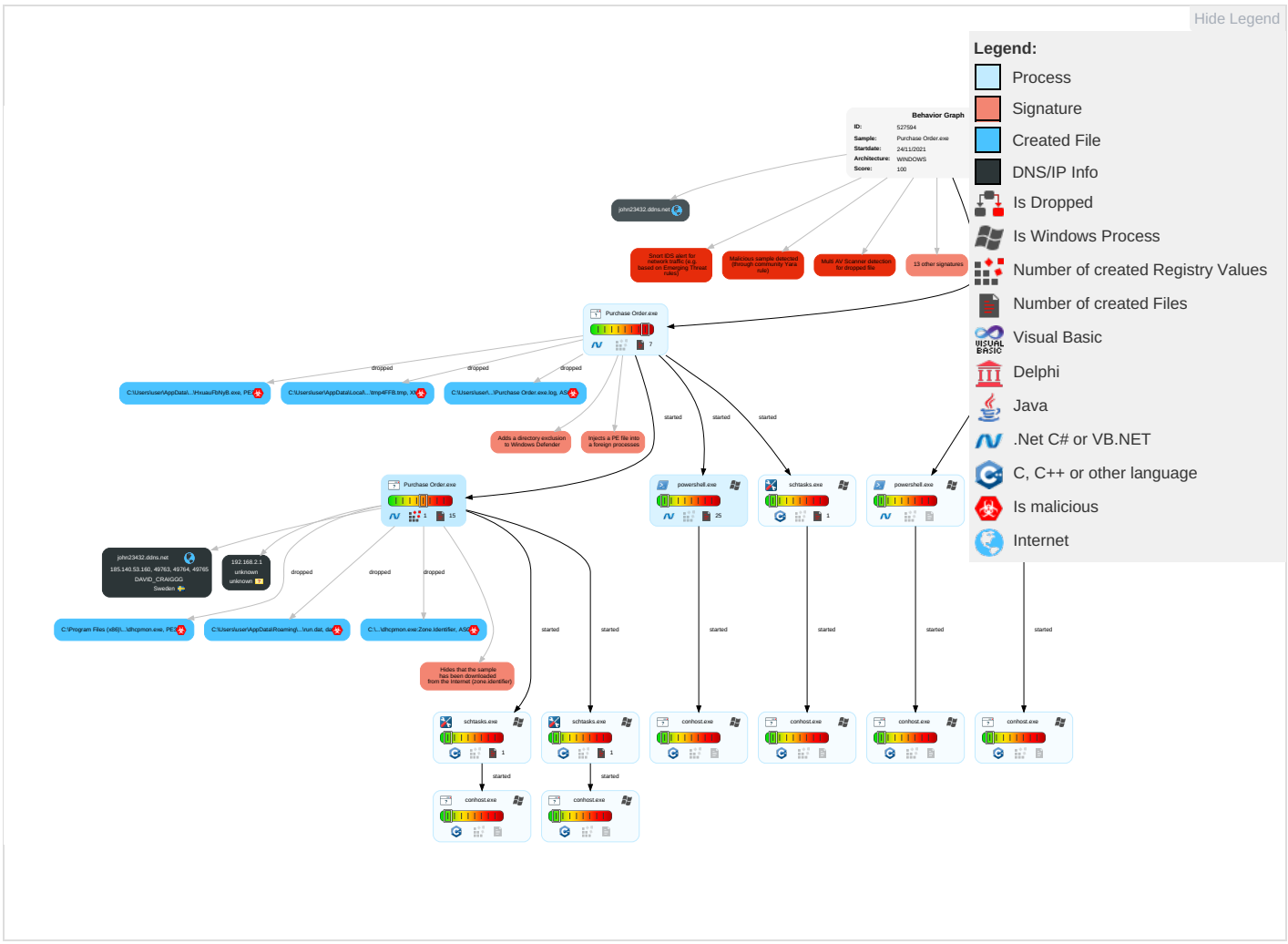
Detected Nanocore Rat

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
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 2	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 2 1 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

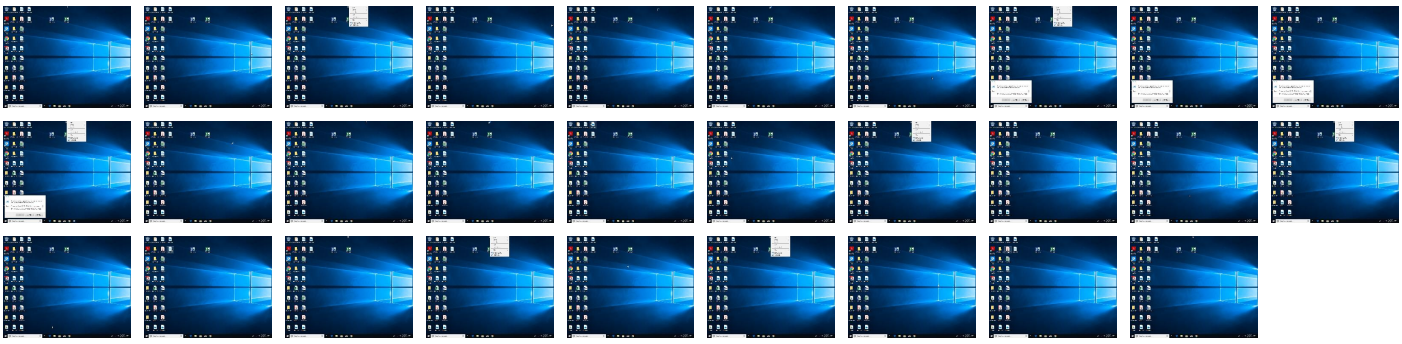
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	
C:\Users\user\AppData\Roaming\HxuauFbNyB.exe	20%	ReversingLabs	ByteCode-MSIL.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.0.Purchase Order.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.Purchase Order.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.0.Purchase Order.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.0.Purchase Order.exe.400000.6.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.Purchase Order.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.2.Purchase Order.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
22.0.Purchase Order.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.Purchase Order.exe.400000.12.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.Purchase Order.exe.400000.10.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
22.0.Purchase Order.exe.400000.8.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.Purchase Order.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.Purchase Order.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.chinhdo.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
john23432.ddns.net	185.140.53.160	true	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.160	john23432.ddns.net	Sweden		209623	DAVID_CRAIGGG	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	527594
Start date:	24.11.2021
Start time:	01:47:08

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Purchase Order.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:	38
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@33/23@16/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 83.8% • Quality standard deviation: 1.2%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
01:48:04	API Interceptor	876x Sleep call for process: Purchase Order.exe modified
01:48:08	API Interceptor	121x Sleep call for process: powershell.exe modified
01:48:17	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
01:48:18	Task Scheduler	Run new task: DHCP Monitor path: "C:\Users\user\Desktop\Purchase Order.exe" s>$(Arg0)
01:48:20	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)
01:48:24	API Interceptor	3x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	441856
Entropy (8bit):	7.870842594798707
Encrypted:	false
SSDEEP:	6144:zLkLojuk0QX5ni5pF/+fucpLL2Iu6va9Lzpqwayp503UAd0xqOMpBFxQS/f7mkdY:zALo5pGpZ+HLL2P68LoaDw0xdMYK6vv
MD5:	C7AC272D4CFD98C9D86BFF3B6C3E89D8
SHA1:	A6334818159CC0BAD0A8BA8CC8204685BF5BA7E5
SHA-256:	443C27B78B0FA24AE1131834D0307FA6DA57F1463695FC6480D0D3874D5DCF64
SHA-512:	2EAF931CE595C551757D9FA8F8C4CB30A2A6513AE4BE06E5C9999FAF1C1D8417BF0BCB522990638F95B5666654A78672DF0DC4EF0D1951738F5188267389C4EF
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F..a.....0..... .....@.. ..... .@.....O..... ....H.....text...p.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....`...D.....n...@...X.....0..7.....r...p(.....s.....+.....X....i2..o.....+...*..0.....r...p..(.....9.....(.....s.....s.... .....8.....-...o.....1...o.....]...+.....,...o.....,...o.....+.....,%...o.....,...o....o.....,...o.....+.....,.....o.....X.....i?W.....o .....8.....(!.....,.....o....,.....o.....] ...+.....,....o"...&.....+3.....o.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase Order.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:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order.exe.log	
Process:	C:\Users\user\Desktop\Purchase Order.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:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	unknown

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Purchase Order.exe.log	
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\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22276
Entropy (8bit):	5.602299935017771
Encrypted:	false
SSDEEP:	384:BtCDDq0AALh4FG0zOqMSBKnAjultl+7paeQ99gt/cxeT1MaXZlbAV7WVIUQeZBDM:a4FGx4KAClthtat8t9C+fwCZVM
MD5:	F3AFDE9F3255078A87DF08B181BCC07B
SHA1:	B6E580C1B2BDE3C6AE08B4B534E804E96661F333
SHA-256:	1E0273C349E6347A208401FB265C89F6BCFFA79BC9ECA55C99EAC682A6F9EE7F
SHA-512:	DECD868CD8A7443050E745A5438DB794DCF7DD2693B0B93595E8A470F5C2C2975448FCF13501D751B169BAD6CBBD2D13B2E700ED06F29823958FA9BAFC2718
Malicious:	false
Reputation:	unknown
Preview:	@...e.....y.....y.o.o...P.....u.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f.....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....System.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1.....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ag4apfai.vhh.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(A
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ag4apfai.vhh.psm1	
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_eg0ibh2b.kqt.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_gmus0usj.be1.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 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_qdvinvb5.qqw.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r1wqq1el.sjv.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_r1wqq1el.sjv.psm1	
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_zlq4x5d5.t3t.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(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp4FFB.tmp	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1597
Entropy (8bit):	5.1421671465980845
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtazxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTEv
MD5:	46DC76C9149F076A473473464AE3C03B
SHA1:	8F929735174899ACDAD9C63121BC06DB79B672B9
SHA-256:	FD81D1D0AF29FC83FE98DB50BAAF9E4B9E1247ABEFF22079AF23B160971780A1
SHA-512:	38E569D2BBBF6549899F300432D0FAC95E12DF4CDFDBA4C86B494E2620B228BDD622ED9FBAE6D1EF8EB0B030A61D60C9CFE1A79A0014079A8C6850B783D5FD6
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmp65C6.tmp	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1304
Entropy (8bit):	5.092592834119789
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0YKDxtn:cbk4oL600QydbQxIYODOLedq34j
MD5:	5819E320692EF4D03DD50A326FF0B6C3
SHA1:	5D43319A1772A63C5BE9612179067BAB1F5C5248
SHA-256:	EE49351DA4C9BDD99685C72B19F8AE36B3391430D6A813A9967C13902A8ED959
SHA-512:	0FCD5D29F893DCC0A3E1854C0BC42868A740D0C9D99DCB360F4BF87970DBD1673EF7F4024862E762B631A90DAA2170A5ADF3B5B62AE33646E97168555D4FE3E1
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmp65C6.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp6E05.tmp	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.109425792877704
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0R3xtn:cbk4oL600QydbQxIYODOLedq3S3j
MD5:	5C2F41CFC6F988C859DA7D727AC2B62A
SHA1:	68999C85FC7E37BAB9216E0099836D40D4545C1C
SHA-256:	98B6E66B6C2173B9B91FC97FE51805340EFDE978B695453742EBAB631018398B
SHA-512:	B5DA5DA378D038AFBF8A7738E47921ED39F9B726E2CAA2993D915D9291A3322F94EFE8CCA6E7AD678A670DB19926B22B20E5028460FCC89CEA7F6635E755733
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmpAF9F.tmp	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1597
Entropy (8bit):	5.1421671465980845
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtazxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTEv
MD5:	46DC76C9149F076A473473464AE3C03B
SHA1:	8F929735174899ACDAD9C63121BC06DB79B672B9
SHA-256:	FD81D1D0AF29FC83FE98DB50BAAF9E4B9E1247ABEFF22079AF23B160971780A1
SHA-512:	38E569D2BBBF6549899F300432D0FAC95E12DF4CDFDBA4C86B494E2620B228BDD622ED9FBAE6D1EF8EB0B030A61D60C9CFE1A79A0014079A8C6850B783D5FD D6
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Local\Temp\tmpB24F.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1597
Entropy (8bit):	5.1421671465980845
Encrypted:	false
SSDEEP:	24:2di4+S2qh/S1KTy1moCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtazxvn:cgeKwYrFdOFzOzN33ODOiDdKrsuTEv
MD5:	46DC76C9149F076A473473464AE3C03B
SHA1:	8F929735174899ACDAD9C63121BC06DB79B672B9
SHA-256:	FD81D1D0AF29FC83FE98DB50BAAF9E4B9E1247ABEFF22079AF23B160971780A1
SHA-512:	38E569D2BBBF6549899F300432D0FAC95E12DF4CDFDBA4C86B494E2620B228BDD622ED9FBAE6D1EF8EB0B030A61D60C9CFE1A79A0014079A8C6850B783D5FD D6
Malicious:	false
Reputation:	unknown

C:\Users\user\AppData\Local\Temp\tmpB24F.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\Purchase Order.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:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35EA5
Malicious:	false
Reputation:	unknown
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\Purchase Order.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:wyy:wyy
MD5:	15C5AF8ECD5BE1F5A50A1EDDE5FEC64D
SHA1:	8DF9D8352484F38F356D0C15FBE3D746BD671DD2
SHA-256:	9D2D45927E7408FEFC468A8D1994C9DF9141E1474CCD20061255E6C0E446FC61
SHA-512:	07A873C5BCD258F844FCDDC047B038D989BA8200232A36B12C611BF64EE5ED56C8AAC971B9DA4BFA88DF243647E749493EDF5F1D82C497FA01D5EC24E98BA02
Malicious:	**true**
Reputation:	unknown
Preview:	..,...H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	data
Category:	modified
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
Reputation:	unknown
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\Purchase Order.exe
File Type:	data
Category:	dropped
Size (bytes):	327432

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

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	41
Entropy (8bit):	4.156061152695156
Encrypted:	false
SSDEEP:	3:oNt+WfW1QK4q6:oNwvaND
MD5:	A5B5387115236B6A3DE7EA168E729F33
SHA1:	424D27EBFDE15D896B9C9FF521FAF694BD182C1E
SHA-256:	218F6E3E727B206A0513EEBD2D82058AC3DFFA441E9EA96DA3A6291232C75C26
SHA-512:	FBB788C650B3F4693F0DF27844D2B6C826F6E3BEE551B2873B26C0A94E8F2AF8861CCE86759B4B5BEC18AEC1C64A902DE34AF48F9AA1C404D776D3EDD1ED5E 24
Malicious:	false
Reputation:	unknown
Preview:	C:\Users\user\Desktop\Purchase Order.exe

C:\Users\user\AppData\Roaming\HxuauFbNyB.exe	
Process:	C:\Users\user\Desktop\Purchase Order.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	441856
Entropy (8bit):	7.870842594798707
Encrypted:	false
SSDEEP:	6144:zLkLojuk0QX5ni5pF/+fucpLL2Iu6va9LzpqwayP503UAd0xqOMpBFxQS/f7mkdY:zALo5pGpZ+HLL2P68LoaDw0xdMYK6vv
MD5:	C7AC272D4CFD98C9D86BFF3B6C3E89D8
SHA1:	A6334818159CC0BAD0A8BA8CC8204685BF5BA7E5
SHA-256:	443C27B78B0FA24AE1131834D0307FA6DA57F1463695FC6480D0D3874D5DCF64
SHA-512:	2EAF931CE595C551757D9FA8F8C4CB30A2A6513AE4BE06E5C9999FAF1C1D8417BF0BCB522990638F95B5666654A78672DF0DC4EF0D1951738F5188267389C4EF
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F..a.....0..... .....@.. ..... .@.....O..... ....H.....text...p.... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....`...D.....n...@...X.....0..7.....r...p(.....s.....+.....X....i2..o.....+...*..0.....r...p..(.....9.....(.....s.....s.... .....8.....-...o.....1...o.....]...+.....,...o.....,...o.....+.....,%...o.....,....o....o.....,..o.....+.....,.....o.....X.....i?W.....o .....8.....(!.....,....o...,....o....] ...+.....,....o"...&.....+3.....o.....

C:\Users\user\AppData\Roaming\HxuauFbNyB.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Purchase Order.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

C:\Users\user\AppData\Roaming\HxuauFbNyB.exe:Zone.Identifier	
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211124\PowerShell_transcript.114127.krYYAnYC.20211124014807.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5789
Entropy (8bit):	5.396216056818636
Encrypted:	false
SSDEEP:	96:BZojUNlqDo1ZoZhjUNlqDo1ZUWg+jZljUNlqDo1ZAruuaZ1:H
MD5:	1BE0A7538B4771C4ECEC66F7E6ECD744
SHA1:	F1CADB0F4F73F6620B85AFA8DD04DDE1EB8D06B2
SHA-256:	524C0FE45543198E3AE9665C1727449495F618D8E4F7D1DBD91F464C7776B7E9
SHA-512:	EF7ADE057FAFEF322A3C653860A563E8AE9079D608F1F2213C2042F04ECBC7122A2800EA8570BB09DC29608023F39ACAEE54039A7B9AD60BBA40B6EE61309ED F
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211124014808..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 114127 (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\HxuauFbNyB.exe..Process ID: 4544..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: 20211124014808..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppDat a\Roaming\HxuauFbNyB.exe..**********..Windows PowerShell transcript start..Start time: 20211124015121..Username: computer\user..RunAs User: computer \jone

C:\Users\user\Documents\20211124\PowerShell_transcript.114127.qKjRv7Ar.20211124014823.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5789
Entropy (8bit):	5.397459798230612
Encrypted:	false
SSDEEP:	96:BZujUNB3qDo1ZuZdjUNB3qDo1ZHWg+jZ+jUNB3qDo1ZlruutZi:p
MD5:	18AD7F9C00F426BCD5C2FB4CDE8AE949
SHA1:	D4BF5C55458901E02119A661CC99A58A4FA3BF71
SHA-256:	94EEAB0F4E488C64853FE46EE49F1D4E8F7DC08A73BBA4F8C590945D6ED834B0
SHA-512:	A6B0BDCDCE67FBC62EDB2226DB8AC015A208537FE0F9DC1FDCA3240B836E6E30FF822E952928BE1E97F939B6648BC9C8FBDE6023929F55BDAE05BD55165F2E D7
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211124014824..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 114127 (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\HxuauFbNyB.exe..Process ID: 5684..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: 20211124014824..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppDat a\Roaming\HxuauFbNyB.exe..**********..Windows PowerShell transcript start..Start time: 20211124015143..Username: computer\user..RunAs User: computer \jone

C:\Users\user\Documents\20211124\PowerShell_transcript.114127.ryLJLjRl.20211124014835.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):	0
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	96:BZ7jUNHqDo1ZNZ+jUNHqDo1Z0FWg+jZLjUNHqDo1Z/ruu/Z8:a
MD5:	169B9794ED2D8F49F3B13E302807E66B
SHA1:	E92AF7E450982DB827344E87E152709DC8F1F906
SHA-256:	50F05A4B39001C72AA4E1FFCE149126F0DC07CDD9222BEBC6A38C3833E74D3CB
SHA-512:	08C0251D3DE4422E79680C6EE90FCFCA3B59D89004B6FB5C96C658F79DB6CCA997ADB016AB1531CAA1A11A92CABEE5AB4A374DE670874573D67C100E3EF92A F6
Malicious:	false
Reputation:	unknown

C:\Users\user\Documents\20211124\PowerShell_transcript.114127.ryLJLjRl.20211124014835.txt	
Preview:	**********..Windows PowerShell transcript start..Start time: 20211124014836..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 114127 (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\HxuauFbNyB.exe..Process ID: 4780..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: 20211124014836..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\HxuauFbNyB.exe..**********..Windows PowerShell transcript start..Start time: 20211124015218..Username: computer\user..RunAs User: computer\jone

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.870842594798707
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Purchase Order.exe
File size:	441856
MD5:	c7ac272d4cfd98c9d86bff3b6c3e89d8
SHA1:	a6334818159cc0bad0a8ba8cc8204685bf5ba7e5
SHA256:	443c27b78b0fa24ae1131834d0307fa6da57f1463695fc6480d0d3874d5dcf64
SHA512:	2eaf931ce595c551757d9fa8f8c4cb30a2a6513ae4be06e5c9999faf1c1d8417bf0bcb522990638f95b5666654a78672df0dc4ef0d1951738f5188267389c4ef
SSDEEP:	6144:zLkLojuk0QX5ni5pF/+fucpLL2Iu6va9Lzpqwayp503UAd0xqOMpBFxQS/f7mkdY:zALo5pGpZ+HLL2P68LoaDw0xdMYK6vv
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F..a.....0..... ....@.. .....@.....

File Icon

Icon Hash:	d092989898a8a488

Static PE Info

General

Entrypoint:	0x46bbea
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:	0x619D8146 [Wed Nov 24 00:03:18 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x69c70	0x69e00	False	0.918471443329	data	7.90563498094	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6c000	0x1bd0	0x1c00	False	0.280970982143	data	3.91574364935	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6e000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-01:48:21.223022	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	54531	8.8.8.8	192.168.2.4
11/24/21-01:48:21.466020	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49763	6640	192.168.2.4	185.140.53.160
11/24/21-01:48:27.757393	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49714	8.8.8.8	192.168.2.4
11/24/21-01:48:27.917802	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49764	6640	192.168.2.4	185.140.53.160
11/24/21-01:48:33.826635	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	58028	8.8.8.8	192.168.2.4
11/24/21-01:48:33.987751	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49765	6640	192.168.2.4	185.140.53.160
11/24/21-01:48:40.104132	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49768	6640	192.168.2.4	185.140.53.160
11/24/21-01:48:47.223646	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49769	6640	192.168.2.4	185.140.53.160
11/24/21-01:48:55.437215	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49910	8.8.8.8	192.168.2.4
11/24/21-01:48:55.610091	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49770	6640	192.168.2.4	185.140.53.160
11/24/21-01:49:01.587828	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	55854	8.8.8.8	192.168.2.4
11/24/21-01:49:01.759606	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49771	6640	192.168.2.4	185.140.53.160
11/24/21-01:49:09.908785	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49785	6640	192.168.2.4	185.140.53.160
11/24/21-01:49:16.338053	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49807	6640	192.168.2.4	185.140.53.160
11/24/21-01:49:22.454612	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49813	6640	192.168.2.4	185.140.53.160
11/24/21-01:49:29.843392	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49815	6640	192.168.2.4	185.140.53.160
11/24/21-01:49:36.198569	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	51255	8.8.8.8	192.168.2.4
11/24/21-01:49:36.362823	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49822	6640	192.168.2.4	185.140.53.160
11/24/21-01:49:43.220874	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	61522	8.8.8.8	192.168.2.4
11/24/21-01:49:43.674432	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49839	6640	192.168.2.4	185.140.53.160
11/24/21-01:49:51.504844	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49841	6640	192.168.2.4	185.140.53.160

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/24/21-01:49:58.390026	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49842	6640	192.168.2.4	185.140.53.160
11/24/21-01:50:05.396906	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49843	6640	192.168.2.4	185.140.53.160

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 01:48:21.116089106 CET	192.168.2.4	8.8.8.8	0x8292	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:27.737557888 CET	192.168.2.4	8.8.8.8	0xf1bc	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:33.804887056 CET	192.168.2.4	8.8.8.8	0x8b20	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:39.916049004 CET	192.168.2.4	8.8.8.8	0xc74a	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:47.006759882 CET	192.168.2.4	8.8.8.8	0xd4cc	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:55.415853024 CET	192.168.2.4	8.8.8.8	0x5327	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:01.566258907 CET	192.168.2.4	8.8.8.8	0xc747	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:08.956610918 CET	192.168.2.4	8.8.8.8	0x1ef3	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:16.159749985 CET	192.168.2.4	8.8.8.8	0xcc44	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:22.270036936 CET	192.168.2.4	8.8.8.8	0xfe0	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:29.518810034 CET	192.168.2.4	8.8.8.8	0x76f3	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:36.176769018 CET	192.168.2.4	8.8.8.8	0xe73b	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:43.199615002 CET	192.168.2.4	8.8.8.8	0x6274	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:51.222964048 CET	192.168.2.4	8.8.8.8	0x2680	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:58.212694883 CET	192.168.2.4	8.8.8.8	0x91bd	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)
Nov 24, 2021 01:50:05.221136093 CET	192.168.2.4	8.8.8.8	0x383	Standard query (0)	john23432.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 01:48:21.223021984 CET	8.8.8.8	192.168.2.4	0x8292	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:27.757392883 CET	8.8.8.8	192.168.2.4	0xf1bc	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:33.826634884 CET	8.8.8.8	192.168.2.4	0x8b20	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:39.935769081 CET	8.8.8.8	192.168.2.4	0xc74a	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:47.024657965 CET	8.8.8.8	192.168.2.4	0xd4cc	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:48:55.437215090 CET	8.8.8.8	192.168.2.4	0x5327	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 01:49:01.587827921 CET	8.8.8.8	192.168.2.4	0xc747	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:08.976273060 CET	8.8.8.8	192.168.2.4	0x1ef3	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:16.179430008 CET	8.8.8.8	192.168.2.4	0xcc44	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:22.289854050 CET	8.8.8.8	192.168.2.4	0xfe0	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:29.537528038 CET	8.8.8.8	192.168.2.4	0x76f3	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:36.198569059 CET	8.8.8.8	192.168.2.4	0xe73b	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:43.220874071 CET	8.8.8.8	192.168.2.4	0x6274	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:51.242897987 CET	8.8.8.8	192.168.2.4	0x2680	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:49:58.232973099 CET	8.8.8.8	192.168.2.4	0x91bd	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)
Nov 24, 2021 01:50:05.240629911 CET	8.8.8.8	192.168.2.4	0x383	No error (0)	john23432.ddns.net		185.140.53.160	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Purchase Order.exe PID: 6284 Parent PID: 5216

General

Start time:	01:47:57
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase Order.exe"
Imagebase:	0x260000
File size:	441856 bytes
MD5 hash:	C7AC272D4CFD98C9D86BFF3B6C3E89D8
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: 00000000.00000002.687313055.0000000003639000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.687313055.0000000003639000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.687313055.0000000003639000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.686415706.0000000002631000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 4544 Parent PID: 6284

General

Start time:	01:48:06
Start date:	24/11/2021
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\HxuauFbNyB.exe
Imagebase:	0x970000
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

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6792 Parent PID: 4544

General

Start time:	01:48:07
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6816 Parent PID: 6284

General

Start time:	01:48:07
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HxuauFbNyB" /XML "C:\Users\user\AppData\Local\Temp\tmp4FFB.tmp
Imagebase:	0x2a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5664 Parent PID: 6816

General

Start time:	01:48:08
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Purchase Order.exe PID: 3416 Parent PID: 6284

General

Start time:	01:48:08
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order.exe
Imagebase:	0x4a0000
File size:	441856 bytes

MD5 hash:	C7AC272D4CFD98C9D86BFF3B6C3E89D8
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: 00000009.00000000.677601605.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.677601605.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.677601605.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.676727006.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.676727006.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.676727006.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000009.00000003.885280898.000000000460D000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.677116035.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.677116035.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.677116035.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.918566646.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.918566646.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.918566646.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.676067039.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.676067039.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.676067039.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: schtasks.exe PID: 5280 Parent PID: 3416

General

Start time:	01:48:16
Start date:	24/11/2021

Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp65C6.tmp
Imagebase:	0x2a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 7064 Parent PID: 5280

General

Start time:	01:48:17
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 7044 Parent PID: 3416

General

Start time:	01:48:18
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp6E05.tmp
Imagebase:	0x2a0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: Purchase Order.exe PID: 7052 Parent PID: 968

General

Start time:	01:48:18
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Purchase Order.exe" 0
Imagebase:	0x610000
File size:	441856 bytes
MD5 hash:	C7AC272D4CFD98C9D86BFF3B6C3E89D8
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: 0000000E.00000002.726406872.0000000003929000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.726406872.0000000003929000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.726406872.0000000003929000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000E.00000002.722519255.0000000002921000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 7072 Parent PID: 7044

General

Start time:	01:48:18
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 1440 Parent PID: 968

General

Start time:	01:48:20
Start date:	24/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true

Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0
Imagebase:	0x280000
File size:	441856 bytes
MD5 hash:	C7AC272D4CFD98C9D86BFF3B6C3E89D8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000010.00000002.715620256.0000000002881000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 20%, ReversingLabs
Reputation:	low

Analysis Process: powershell.exe PID: 5684 Parent PID: 7052

General

Start time:	01:48:22
Start date:	24/11/2021
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\HxuauFbNyB.exe
Imagebase:	0x970000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 5628 Parent PID: 5684

General

Start time:	01:48:23
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5712 Parent PID: 7052

General

Start time:	01:48:23
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\HxuauFbNyB" /XML "C:\Users\user\AppData\Local\Temp\tmpAF9F.tmp
Imagebase:	0x2a0000

File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 4240 Parent PID: 5712

General

Start time:	01:48:24
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: dhcpmon.exe PID: 5248 Parent PID: 3424

General

Start time:	01:48:25
Start date:	24/11/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	"C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe"
Imagebase:	0x980000
File size:	441856 bytes
MD5 hash:	C7AC272D4CFD98C9D86BFF3B6C3E89D8
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: 00000015.00000002.743570227.0000000003E19000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.743570227.0000000003E19000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.743570227.0000000003E19000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000015.00000002.742127513.0000000002E11000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: Purchase Order.exe PID: 5600 Parent PID: 7052

General

Start time:	01:48:25
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\Purchase Order.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Purchase Order.exe

Imagebase:	0x750000
File size:	441856 bytes
MD5 hash:	C7AC272D4CFD98C9D86BFF3B6C3E89D8
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: 00000016.00000000.714576190.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000000.714576190.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000000.714576190.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000000.715150890.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000000.715150890.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000000.715150890.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000000.715695087.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000000.715695087.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000000.715695087.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000002.737893827.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.737893827.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.737893827.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.740418253.0000000002AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.740418253.0000000002AF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.740872002.0000000003AF9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.740872002.0000000003AF9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000016.00000000.713969209.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000000.713969209.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000000.713969209.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: powershell.exe PID: 4780 Parent PID: 5248

General

Start time:	01:48:33
Start date:	24/11/2021
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\HxuauFbNyB.exe
Imagebase:	0x970000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true

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

Disassembly

Code Analysis