ID: 528201
Sample Name: TS#U007e039873663-30987637393.exe
Cookbook: default.jbs
Time: 20:56:08
Date: 24/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

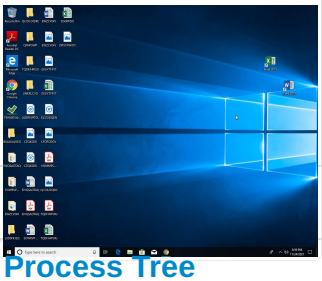
Windows Analysis Report TS#U007e039873663-3098763…

Overview

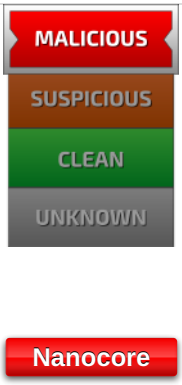
General Information

Sample Name:	TS#U007e039873663-30987637393.exe
Analysis ID:	528201
MD5:	23a2d703d27e7b..
SHA1:	c8bf9a5ff9b1c53…
SHA256:	4ae669ec3635f90.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

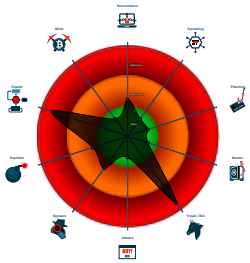


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Yara detected AntiVM3
- Detected Nanocore Rat
- Multi AV Scanner detection for dropp…
- Yara detected Nanocore RAT
- Sigma detected: Bad Opsec Default…
- Tries to detect sandboxes and other…
- Sigma detected: Suspicius Add Tas…
- .NET source code contains potentia…

Classification



Process Tree

- **System is w10x64**
- TS#U007e039873663-30987637393.exe (PID: 5300 cmdline: "C:\Users\user\Desktop\TS#U007e039873663-30987637393.exe" MD5: 23A2D703D27E7BE5248EA4498790681F)
  - powershell.exe (PID: 5220 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\KwxdAPDG.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 4228 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KwxdAPDG" /XML "C:\Users\user\AppData\Local\Temp\tmp1099.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6148 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RegSvcs.exe (PID: 6212 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - schtasks.exe (PID: 6712 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor" /xml "C:\Users\user\AppData\Local\Temp\tmp2D.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6756 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 6824 cmdline: schtasks.exe" /create /f /tn "DHCP Monitor Task" /xml "C:\Users\user\AppData\Local\Temp\tmp790.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
      - conhost.exe (PID: 6832 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- RegSvcs.exe (PID: 6840 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 6876 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 7060 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" 0 MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 7088 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- dhcpmon.exe (PID: 5384 cmdline: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" MD5: 2867A3817C9245F7CF518524DFD18F28)
  - conhost.exe (PID: 1112 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7b578534-8b04-4a5d-9eb5-d375830c",
  "Group": "6262",
  "Domain1": "6262.hopto.org",
  "Domain2": "185.140.53.131",
  "Port": 6262,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task>"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.514411052.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000009.00000002.514411052.000000000040 2000.00000040.00000001.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:$j: #=q
00000009.00000002.514411052.000000000040 2000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000009.00000002.514411052.000000000040 2000.00000040.00000001.sdmp	Nanocore	detect Nanocore in memory	JPCERT/CC Incident Response Group	• 0xfcf5:$v1: NanoCore Client • 0xfd05:$v1: NanoCore Client • 0x115c6:$v2: PluginCommand • 0x115ae:$v3: CommandType
00000009.00000000.284695927.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Click to see the 34 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.2.RegSvcs.exe.5270000.5.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
9.2.RegSvcs.exe.5f90000.7.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
9.2.RegSvcs.exe.5f90000.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
9.2.RegSvcs.exe.5f94629.6.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
9.2.RegSvcs.exe.5f94629.6.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xb184:$x1: NanoCore.ClientPluginHost • 0xb1b1:$x2: IClientNetworkHost
Click to see the 52 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Possible Applocker Bypass

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:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Networking:

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

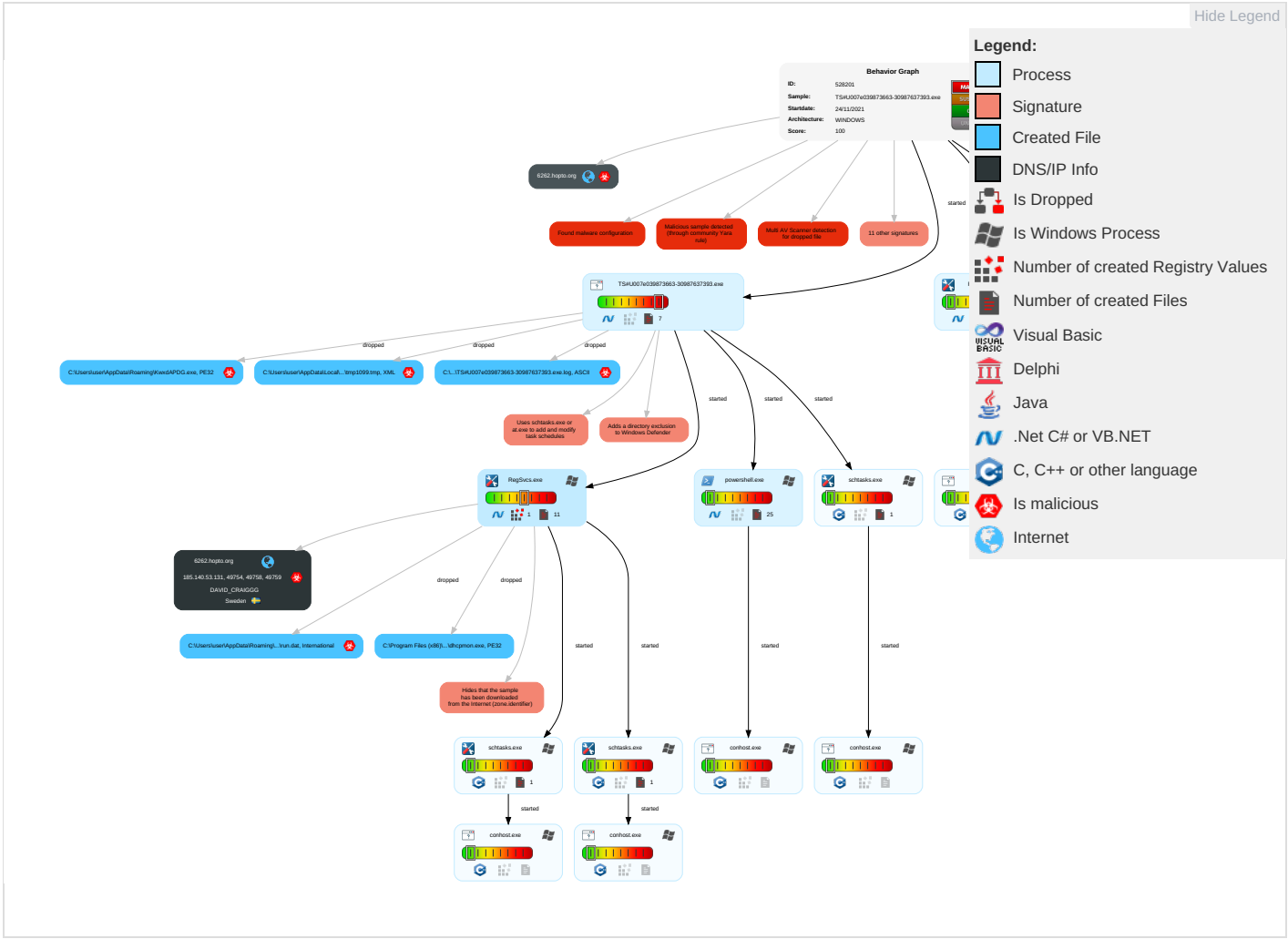
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 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	Eavesdro Insecure Network Commun
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	LSASS Memory	Security Software Discovery 2 1	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit S Redirect Calls/SM
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Remote Access Software 1	Exploit S Track De Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
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	Manipula Device Commun
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue W Access P
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	Downgra Insecure Protocols

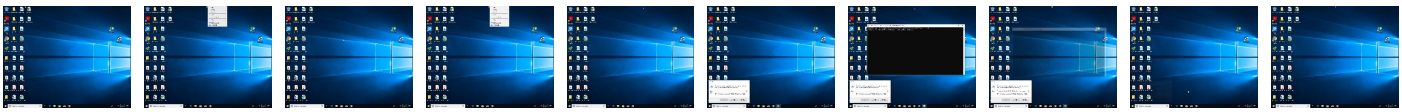
Behavior Graph



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
TS#U007e039873663-30987637393.exe	29%	Virustotal		Browse
TS#U007e039873663-30987637393.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\KwxdAPDG.exe	31%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.RegSvcs.exe.400000.3.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.RegSvcs.exe.5f90000.7.unpack	100%	Avira	TR/NanoCore.fadte		Download File
9.0.RegSvcs.exe.400000.4.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.2.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.1.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
9.2.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
6262.hopto.org	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
6262.hopto.org	2%	Virustotal		Browse
6262.hopto.org	0%	Avira URL Cloud	safe	
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	
185.140.53.131	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
6262.hopto.org	185.140.53.131	true	true	• 2%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
6262.hopto.org	true	• 2%, Virustotal, Browse • Avira URL Cloud: safe	unknown
185.140.53.131	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.131	6262.hopto.org	Sweden		209623	DAVID_CRAIGGG	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528201
Start date:	24.11.2021
Start time:	20:56:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	TS#U007e039873663-30987637393.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:	39
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@21/18@12/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 69% • Quality standard deviation: 34.1%
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:	Show All

Simulations

Behavior and APIs

Time	Type	Description
20:57:17	API Interceptor	2x Sleep call for process: TS#U007e039873663-30987637393.exe modified
20:57:22	API Interceptor	27x Sleep call for process: powershell.exe modified
20:57:31	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
20:57:34	Task Scheduler	Run new task: DHCP Monitor path: "C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe" s>$(Arg0)
20:57:34	API Interceptor	834x Sleep call for process: RegSvcs.exe modified
20:57:36	Task Scheduler	Run new task: DHCP Monitor Task path: "C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe" s>$(Arg0)

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.131	ERIG_0983763673-093876536783.exe	Get hash	malicious	Browse	
	tj9KzQvUFy.exe	Get hash	malicious	Browse	
	TR0398734893 50601251.exe	Get hash	malicious	Browse	
	UTYHFG03983765367839837653.exe	Get hash	malicious	Browse	
	XPDL_0938763673-3987356378998736563.exe	Get hash	malicious	Browse	
	HVX_098765434567-5456799876.exe	Get hash	malicious	Browse	
	DFTE98765464-4987465546784.exe	Get hash	malicious	Browse	
	MB#U007e1234567876-098767.exe	Get hash	malicious	Browse	
	IMG#U007e0398763536783.exe	Get hash	malicious	Browse	
	remitcopy.jar	Get hash	malicious	Browse	
	remittance copy.jar	Get hash	malicious	Browse	
	remittance copy.jar	Get hash	malicious	Browse	
	MRC20201030XMY,pdf.exe	Get hash	malicious	Browse	
	SP AIR B00,pdf.exe	Get hash	malicious	Browse	
	FACA000400007998.pdf.exe	Get hash	malicious	Browse	
	MS210201,pdf.exe	Get hash	malicious	Browse	
	20082020141903,pdf.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	
	PROOF OF PAYMENT.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
6262.hopto.org	ERIG_0983763673-093876536783.exe	Get hash	malicious	Browse	• 185.140.53.131
	tj9KzQvUFy.exe	Get hash	malicious	Browse	• 185.140.53.131

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	ERIG_0983763673-093876536783.exe	Get hash	malicious	Browse	• 185.140.53.131
	copy_tt_inv_10192ne.exe	Get hash	malicious	Browse	• 91.193.75.149
	DHL Tracking.exe	Get hash	malicious	Browse	• 185.140.53.33
	tj9KzQvUFy.exe	Get hash	malicious	Browse	• 185.140.53.131
	Purchase Order.exe	Get hash	malicious	Browse	• 185.140.53.160
	Orden de Compra -SA765443,pdf.exe	Get hash	malicious	Browse	• 185.140.53.12
	purchase order 0112.exe	Get hash	malicious	Browse	• 185.140.53.137
	9mMANDmw9O.exe	Get hash	malicious	Browse	• 91.193.75.190
	TR0398734893 50601251.exe	Get hash	malicious	Browse	• 185.140.53.131
	swift.xls	Get hash	malicious	Browse	• 91.193.75.212
	SOA_0009877890.exe	Get hash	malicious	Browse	• 185.244.30.58
	8UYr1od7iW.exe	Get hash	malicious	Browse	• 91.193.75.148
	928272_Payment_Receipt.vbs	Get hash	malicious	Browse	• 185.140.53.3
	N2K18_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	U2M19O_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	J3m1a_Payment_Copy.vbs	Get hash	malicious	Browse	• 185.140.53.3
	18-11-21 Statement.xlsx	Get hash	malicious	Browse	• 91.193.75.148
	bWKXCwatmt.exe	Get hash	malicious	Browse	• 91.193.75.148
	17-11-21 STATEMENT.xlsx	Get hash	malicious	Browse	• 91.193.75.148
	Copy of Complaint report-1st Nov21 to 16th Nov21.xlsx	Get hash	malicious	Browse	• 91.193.75.148

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	ERIG_0983763673-093876536783.exe	Get hash	malicious	Browse	
	Euro invoice.exe	Get hash	malicious	Browse	
	Shipping Document BL Draft.exe	Get hash	malicious	Browse	
	incorrect payment information.exe	Get hash	malicious	Browse	
	TransactionSummary_22-11-2021.exe	Get hash	malicious	Browse	
	SWIFT COPY.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	TT COPY.exe	Get hash	malicious	Browse	
	Payment Advice 50053945.exe	Get hash	malicious	Browse	
	750845PaymentReceipt.exe	Get hash	malicious	Browse	
	Copy BL and Debit Note.exe	Get hash	malicious	Browse	
	QUOTATION.exe	Get hash	malicious	Browse	
	PO_SBK4128332S.exe	Get hash	malicious	Browse	
	New order - C.S.I No. 0987.exe	Get hash	malicious	Browse	
	Bank payment swift message.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	HSBC Payment Advice.exe	Get hash	malicious	Browse	
	UTYHFG03983765367839837653.exe	Get hash	malicious	Browse	
	qaNcOX8rVf.exe	Get hash	malicious	Browse	
	XPDL_0938763673-3987356378998736563.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	45152
Entropy (8bit):	6.149629800481177
Encrypted:	false
SSDEEP:	768:bBbSoy+SdIBf0k2dsYyV6Iq87PiU9FViaLmf:EoOIBf0ddsYy8LUjVBC
MD5:	2867A3817C9245F7CF518524DFD18F28
SHA1:	D7BA2A111CEDD5BF523224B3F1CFE58EEC7C2FDC
SHA-256:	43026DCFF238F20CFF0419924486DEE45178119CFDD0D366B79D67D950A9BF50
SHA-512:	7D3D3DBB42B7966644D716AA9CBC75327B2ACB02E43C61F1DAD4AFE5521F9FE248B33347DFE15B637FB33EB97CDB322BCAEAE08BAE3F2FD863A9AD9B3A4D(B42
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Joe Sandbox View:	• Filename: ERIG_0983763673-093876536783.exe, Detection: malicious, Browse • Filename: Euro invoice.exe, Detection: malicious, Browse • Filename: Shipping Document BL Draft.exe, Detection: malicious, Browse • Filename: incorrect payment information.exe, Detection: malicious, Browse • Filename: TransactionSummary_22-11-2021.exe, Detection: malicious, Browse • Filename: SWIFT COPY.exe, Detection: malicious, Browse • Filename: TT COPY.exe, Detection: malicious, Browse • Filename: Payment Advice 50053945.exe, Detection: malicious, Browse • Filename: 750845PaymentReceipt.exe, Detection: malicious, Browse • Filename: Copy BL and Debit Note.exe, Detection: malicious, Browse • Filename: QUOTATION.exe, Detection: malicious, Browse • Filename: PO_SBK4128332S.exe, Detection: malicious, Browse • Filename: New order - C.S.I No. 0987.exe, Detection: malicious, Browse • Filename: Bank payment swift message.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: SOA.exe, Detection: malicious, Browse • Filename: HSBC Payment Advice.exe, Detection: malicious, Browse • Filename: UTYHFG03983765367839837653.exe, Detection: malicious, Browse • Filename: qaNcOX8rVf.exe, Detection: malicious, Browse • Filename: XPDL_0938763673-3987356378998736563.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zX.Z.....0..d.....V.... .....@.. .....".. ..`.....O.....8.....r..`>..... ....H.....text...\c... ...d..... ..`.rsrc...8.....f.....@..@.reloc..... .....p.....@..B.....8.....H.....+...S.....|...P.....r...p(....*2.(....(....*z..r...p(....(....(.....}....*..{....*.s.....*.0..{.....Q.-.s.....+i~....o....(..... s.....o.....r!..p..(....Q.P,:.P.....(....o....o .....(....o!...o".....,..o#...t.....*..0..(..... ....s$.....o%....X..(....-..*.o&...*.0.....('.....&.....*.*.....0.....(.....&.....*..... .....0.....(.....(....~....,(....~....o....9]...

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\RegSvcs.exe.log	
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\TS#U007e039873663-30987637393.exe.log	
Process:	C:\Users\user\Desktop\TS#U007e039873663-30987637393.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**
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:	modified
Size (bytes):	142
Entropy (8bit):	5.090621108356562
Encrypted:	false
SSDEEP:	3:QHXMKa/xwwUC7WglAFXMWA2yTMGfsbNRLFS9Am12MFuAvOAsDeieVyn:Q3La/xwczlAFXMWTyAGCDLIP12MUAvvw
MD5:	8C0458BB9EA02D50565175E38D577E35
SHA1:	F0B50702CD6470F3C17D637908F83212FDBDB2F2
SHA-256:	C578E86DB701B9AFA3626E804CF434F9D32272FF59FB32FA9A51835E5A148B53
SHA-512:	804A47494D9A462FFA6F39759480700ECBE5A7F3A15EC3A6330176ED9C04695D2684BF6BF85AB86286D52E7B727436D0BB2E8DA96E20D47740B5CE3F856B5D0F
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.EnterpriseServices, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..

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):	22280
Entropy (8bit):	5.6034160960970265
Encrypted:	false
SSDEEP:	384:7tCD60oQyV04BG0cSBKnsjultIav7Y9ghSJ3xyT1MaDZlbAV7UBYCwu5ZBDI+iq8:d9VRB44KsClt1fhcwC6fwxiV8
MD5:	6C39551AF5B34EC8FEA91DCEB45DAA78
SHA1:	4FA487374BAD31ECAE5C252281906D7FEDBA2CB8
SHA-256:	27D7D1C3B39937C8A79562E69F85E17378BC44EAE65E21B24757A6E58A2101B8
SHA-512:	B2F3EC0F43C56FACA7F1DF05775182BA2294D4046C3A0DFE8E3BB01587A43479AC812C1EA06ED02105FE511DDAB90B48F789003866F28C2C3C926F71ECB3511E
Malicious:	false
Preview:	@...e.....y.....h.[.....J.....@.....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_hbvoiado.dhb.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
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ihvkvlww.uxb.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
Preview:	 1

C:\Users\user\AppData\Local\Temp\tmp1099.tmp	
Process:	C:\Users\user\Desktop\TS#U007e039873663-30987637393.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1599
Entropy (8bit):	5.129523934013168
Encrypted:	false
SSDEEP:	24:2di4+S2qh/a1Kby1moqUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtQxvn:cgeCaYrFdOFzOzN33ODOiDdKrsuTgv
MD5:	634ED616FA8C228A3DD6819AAF2AF4EA
SHA1:	3494D974547208CB848D2FFBFCBD182CE7BB7EE9
SHA-256:	4B52E47393630F2785F5E645429CAB819581501DB1257009F24AB2586C2F34D8
SHA-512:	769123AEE13B0DAFC5958AB1F5EE14E7EC90D0ECF02166ED5A1A39BC41303CBE6FBC2F1B4DD50053666F81172922FE5445852F94F377769B3E89CDF94AC6EFE 2
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>.

C:\Users\user\AppData\Local\Temp\tmp2D.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1320
Entropy (8bit):	5.135668813522653
Encrypted:	false
SSDEEP:	24:2dH4+S/4oL600QlMhEMjn5pwjVLUYODOLG9RJh7h8gK0mXxtn:cbk4oL600QydbQxIYODOLedq3ZXj
MD5:	8CAD1B41587CED0F1E74396794F31D58
SHA1:	11054BF74FCF5E8E412768035E4DAE43AA7B710F
SHA-256:	3086D914F6B23268F8A12CB1A05516CD5465C2577E1D1E449F1B45C8E5E8F83C
SHA-512:	99C2EF89029DE51A866DF932841684B7FC912DF21E10E2DD0D09E400203BBDC6CBA6319A31780B7BF8B286D2CEA8EA3FC7D084348BF2F002AB4F5A34218CCB F

C:\Users\user\AppData\Local\Temp\tmp2D.tmp	
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Local\Temp\tmp790.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.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
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo />.. <Triggers />.. <Principals>.. <Principal id="Author">.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>HighestAvailable</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>.. <AllowHardTerminate>true</AllowHardTerminate>.. <StartWhenAvailable>false</StartWhenAvailable>.. <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>.. <IdleSettings>.. <StopOnIdleEnd>false</StopOnIdleEnd>.. <RestartOnIdle>false</RestartOnIdle>.. </IdleSettings>.. <AllowStartOnDemand>true</AllowStartOnDemand>.. <Enabled>true</Enabled>.. <Hidden>false</Hidden>.. <RunOnlyIfIdle>false</RunOnlyIfIdle>.. <Wak

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	International EBCDIC text, with NEL line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:nA8:T
MD5:	0A931E58D0C6C1FA2D7587F9B6E78A09
SHA1:	B4F8357B3A82C206197CD51B3CE0219425B46676
SHA-256:	4CB5E0D755B6C97A9D423862B6F56539B67F67FA289598A7A30CFCDD48017C73
SHA-512:	3A5ED778A7ECC5BEFD2A51052745AB1E9F22BE4606C50265856B2C7924D32F889EED21ABFB9A88DBFBD27A155ABB3C5A79A77AF5A18830EA554F620BEBE4D9B2
Malicious:	**true**
Preview:	.p....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\task.dat	
Process:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	57
Entropy (8bit):	4.830795005765378
Encrypted:	false
SSDEEP:	3:oMty8WddSWA1KMNn:oMLW6WA1j
MD5:	08E799E8E9B4FDA648F2500A40A11933
SHA1:	AC76B5E20DED247803448A2F586731ED7D84B9F3
SHA-256:	D46E34924067EB071D1F031C0BC015F4B711EDCE64D8AE00F24F29E73ECB71DB
SHA-512:	5C5701A86156D573BE274E73615FD6236AC89630714863A4CB2639EEC8EC1BE746839EBF8A9AEBA0A9BE326AF6FA02D8F9BD7A93D3FFB139BADE945572DF5FE9
Malicious:	false
Preview:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe

C:\Users\user\AppData\Roaming\KwxdAPDG.exe	
Process:	C:\Users\user\Desktop\TS#U007e039873663-30987637393.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows

C:\Users\user\AppData\Roaming\KwxdAPDG.exe	
Category:	dropped
Size (bytes):	629248
Entropy (8bit):	7.130547868396553
Encrypted:	false
SSDEEP:	12288:bWXN/LqM8Djpe7F035txKRUiMYRTAjxSwAS/r3q3WGXWe:9MIeG3geIR5ur3hGXWe
MD5:	23A2D703D27E7BE5248EA4498790681F
SHA1:	C8BF9A5FF9B1C53CCF51D575E3B6B31973FBF669
SHA-256:	4AE669EC3635F90DC720819CC42BE0A400C431076177F5AD0BFB4867785588CC
SHA-512:	2EFF5AF7586A3C6D6BBDCF7962F6C6117F7128BC86910B4E6DB26F55CA1C7107B799BD3DDB4AF50C113D463CA94EFADB06814910B58FB13A9CE7E268046D136
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 31%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}.a..... .....@.. .....@.....W..... ....H.....text..... ....`.rsrc.....@..@.reloc..... .....@..B.....H.....=.....p...(y.....z.(.....}.....(....o....}....*..0.....{.....3.....(.....*.....0.....{.....,....f.....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....og...:q....(....+..(.....}.....(.....*.....n..}.....{...,..{....o^...*..{....*.s..

C:\Users\user\AppData\Roaming\KwxdAPDG.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\TS#U007e039873663-30987637393.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:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211124\PowerShell_transcript.494126.hfHaKU58.20211124205720.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):	5791
Entropy (8bit):	5.387561753134428
Encrypted:	false
SSDEEP:	96:BZn/6N9qDo1ZjvZ9/6N9qDo1ZGKQyjZQ/6N9qDo1ZGnCChZm:x
MD5:	47BCF2434D1F83F1C84432B3DE202643
SHA1:	ECD620DEAB30E677D86817546E0722BB6554D76B
SHA-256:	C0FFE7E9A35FA5E549F2E0F429A978A0BE4C5B69AF25CB90BC0FDFFA3032A6E8
SHA-512:	0AC5D1B7C0594BCB94D23D53F4A06913D1DEF83D8772573665FB7E152D4E841B5E78C9E8EA882A44E51842981E65C211AC891F6E889310FD09E59A0909705805
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211124205722..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 494126 (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\KwxdAPDG.exe..Process ID: 5220..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: 20211124205722..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\KwxdAPDG.exe..**********..Windows PowerShell transcript start..Start time: 20211124210047..Username: computer\user..RunAs User: computer\alf

\Device\ConDrv	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1141
Entropy (8bit):	4.44831826838854
Encrypted:	false
SSDEEP:	24:zKLXkb4DObntKlglUEnfQtvNuNpKOK5aM9YJC:zKL0b4DQntKKH1MqJC
MD5:	1AEB3A784552CFD2AEDEDC1D43A97A4F
SHA1:	804286AB9F8B3DE053222826A69A7CDA3492411A
SHA-256:	0BC438F4B1208E1390C12D375B6CBB08BF47599D1F24BD07799BB1DF384AA293
SHA-512:	5305059BA86D5C2185E590EC036044B2A17ED9FD9863C2E3C7E7D8035EF0C79E53357AF5AE735F7D432BC70156D4BD3ACB42D100CFB05C2FB669EA22368F141

\Device\ConDrv	
Malicious:	false
Preview:	Microsoft (R) .NET Framework Services Installation Utility Version 4.7.3056.0..Copyright (C) Microsoft Corporation. All rights reserved.....USAGE: regsvcs.exe [options] AssemblyName..Options:.. /? or /help Display this usage message... /fc Find or create target application (default)... /c Create target application, error if it already exists... /exapp Expect an existing application... /tlb:<tlbfile> Filename for the exported type library... /appname:<name> Use the specified name for the target application... /parname:<name> Use the specified name or id for the target partition... /extlb Use an existing type library... /reconfig Re configure existing target application (default)... /noreconfig Don't reconfigure existing target application... /u Uninstall target application... /nologo S uppress logo output... /quiet Suppress logo output and success output... /c

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.130547868396553
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:	TS#U007e039873663-30987637393.exe
File size:	629248
MD5:	23a2d703d27e7be5248ea4498790681f
SHA1:	c8bf9a5ff9b1c53ccf51d575e3b6b31973fbf669
SHA256:	4ae669ec3635f90dc720819cc42be0a400c431076177f5ad0bfb4867785588cc
SHA512:	2eff5af7586a3c6d6bbdcf7962f6c6117f7128bc86910b4e6db26f55ca1c7107b799bd3ddb4af50c113d463ca94efadb06814910b58fb13a9ce7e268046d13a6
SSDEEP:	12288:bWXN/LqM8Djpe7F035txKRUiMYRTAjxSwAS/r3q3WGXWe:9MIeG3geIR5ur3hGXWe
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...}..a..... .....@.. .....@.....

File Icon

Icon Hash:	0cc1a4daca6cb186

Static PE Info

General

Entrypoint:	0x46c7de
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619DC67D [Wed Nov 24 04:58:37 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	0x6a7e4	0x6a800	False	0.917099930311	data	7.90446588697	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x6e000	0x2eda0	0x2ee00	False	0.329864583333	data	4.2437278553	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	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
11/24/21-20:57:35.753798	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49557	8.8.8.8	192.168.2.5
11/24/21-20:57:40.970015	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	52441	8.8.8.8	192.168.2.5
11/24/21-20:57:46.490879	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	62176	8.8.8.8	192.168.2.5
11/24/21-20:58:07.013617	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	56969	8.8.8.8	192.168.2.5
11/24/21-20:58:12.249526	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	49992	8.8.8.8	192.168.2.5
11/24/21-20:58:38.243338	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	50463	8.8.8.8	192.168.2.5
11/24/21-20:59:14.161712	UDP	254	DNS SPOOF query response with TTL of 1 min. and no authority	53	59261	8.8.8.8	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 20:57:35.732611895 CET	192.168.2.5	8.8.8.8	0xda1e	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:57:40.948204994 CET	192.168.2.5	8.8.8.8	0xce6c	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:57:46.467221022 CET	192.168.2.5	8.8.8.8	0x5dca	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:06.991986036 CET	192.168.2.5	8.8.8.8	0x4909	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:12.225630045 CET	192.168.2.5	8.8.8.8	0x75aa	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:17.469953060 CET	192.168.2.5	8.8.8.8	0x40d8	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 24, 2021 20:58:38.221395016 CET	192.168.2.5	8.8.8.8	0x671e	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:43.381181002 CET	192.168.2.5	8.8.8.8	0xed0e	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:48.580826044 CET	192.168.2.5	8.8.8.8	0x245d	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:59:09.022186041 CET	192.168.2.5	8.8.8.8	0x11c6	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:59:14.140676022 CET	192.168.2.5	8.8.8.8	0xebe2	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)
Nov 24, 2021 20:59:19.671153069 CET	192.168.2.5	8.8.8.8	0xa570	Standard query (0)	6262.hopto.org	A (IP address)	IN (0x0001)

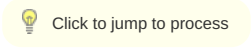
DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 24, 2021 20:57:35.753798008 CET	8.8.8.8	192.168.2.5	0xda1e	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:57:40.970015049 CET	8.8.8.8	192.168.2.5	0xce6c	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:57:46.490879059 CET	8.8.8.8	192.168.2.5	0x5dca	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:07.013617039 CET	8.8.8.8	192.168.2.5	0x4909	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:12.249526024 CET	8.8.8.8	192.168.2.5	0x75aa	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:17.489674091 CET	8.8.8.8	192.168.2.5	0x40d8	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:38.243338108 CET	8.8.8.8	192.168.2.5	0x671e	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:43.399024010 CET	8.8.8.8	192.168.2.5	0xed0e	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:58:48.598551035 CET	8.8.8.8	192.168.2.5	0x245d	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:59:09.042196035 CET	8.8.8.8	192.168.2.5	0x11c6	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:59:14.161711931 CET	8.8.8.8	192.168.2.5	0xebe2	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)
Nov 24, 2021 20:59:19.690610886 CET	8.8.8.8	192.168.2.5	0xa570	No error (0)	6262.hopto.org		185.140.53.131	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: TS#U007e039873663-30987637393.exe PID: 5300 Parent PID: 468

General

Start time:	20:57:08
Start date:	24/11/2021
Path:	C:\Users\user\Desktop\TS#U007e039873663-30987637393.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\TS#U007e039873663-30987637393.exe"
Imagebase:	0x7f0000
File size:	629248 bytes
MD5 hash:	23A2D703D27E7BE5248EA4498790681F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.288365685.0000000002BE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.289219866.0000000003BE9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.289219866.0000000003BE9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.289219866.0000000003BE9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore, Description: detect Nanocore in memory, Source: 00000000.00000002.289219866.0000000003BE9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 5220 Parent PID: 5300

General

Start time:	20:57:19
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\KwxdAPDG.exe
Imagebase:	0x2b0000
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: 2964 Parent PID: 5220

General

Start time:	20:57:20
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 4228 Parent PID: 5300

General

Start time:	20:57:20
Start date:	24/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\KwxdAPDG" /XML "C:\Users\user\AppData\Local\Temp\tmp1099.tmp
Imagebase:	0x13b0000
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: 6148 Parent PID: 4228

General

Start time:	20:57:22
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff797770000
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: RegSvcs.exe PID: 6212 Parent PID: 5300

General

Start time:	20:57:24
Start date:	24/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Imagebase:	0x670000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.514411052.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.514411052.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.514411052.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore, Description: detect Nanocore in memory, Source: 00000009.00000002.514411052.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.284695927.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.284695927.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.284695927.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore, Description: detect Nanocore in memory, Source: 00000009.00000000.284695927.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.286465797.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.286465797.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.286465797.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore, Description: detect Nanocore in memory, Source: 00000009.00000000.286465797.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.285465927.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.285465927.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.285465927.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore, Description: detect Nanocore in memory, Source: 00000009.00000000.285465927.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.524441237.0000000005270000.00000004.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.522878326.0000000003A59000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000002.522878326.0000000003A59000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000000.286097304.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000009.00000000.286097304.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000000.286097304.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: Nanocore, Description: detect Nanocore in memory, Source: 00000009.00000000.286097304.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.524926024.0000000005F90000.00000004.00020000.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.524926024.0000000005F90000.00000004.00020000.sdmp, Author: Florian Roth
Reputation:	high

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: 6712 Parent PID: 6212

General

Start time:	20:57:31
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\tmp2D.tmp
Imagebase:	0x13b0000
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: 6756 Parent PID: 6712

General

Start time:	20:57:32
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 6824 Parent PID: 6212

General

Start time:	20:57:33
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\tmp790.tmp
Imagebase:	0x13b0000
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: 6832 Parent PID: 6824

General

Start time:	20:57:34
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: RegSvcs.exe PID: 6840 Parent PID: 904

General

Start time:	20:57:34
Start date:	24/11/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe 0
Imagebase:	0x740000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: conhost.exe PID: 6876 Parent PID: 6840

General

Start time:	20:57:34
Start date:	24/11/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 7060 Parent PID: 904

General

Start time:	20:57:36
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:	0xcf0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 0%, Metadefender, Browse • Detection: 0%, ReversingLabs

Analysis Process: conhost.exe PID: 7088 Parent PID: 7060

General

Start time:	20:57:37
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: dhcpmon.exe PID: 5384 Parent PID: 3472

General

Start time:	20:57:39
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:	0x7f0000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true

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

Analysis Process: conhost.exe PID: 1112 Parent PID: 5384

General

Start time:	20:57:40
Start date:	24/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis