ID: 358139
Sample Name: cplaMuv3PV.exe
Cookbook: default.jbs
Time: 04:01:25
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

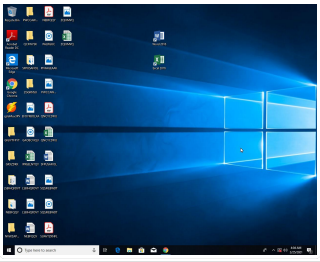
Analysis Report cpIaMuv3PV.exe

Overview

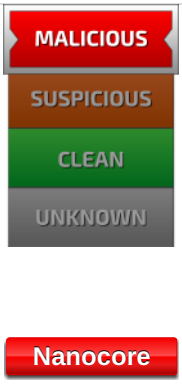
General Information

Sample Name:	cpIaMuv3PV.exe
Analysis ID:	358139
MD5:	a8911878f9c096c..
SHA1:	1dffaac5e83c62a..
SHA256:	498df02f7263a2b..
Tags:	exe NanoCore RAT
Infos:	

Most interesting Screenshot:



Detection



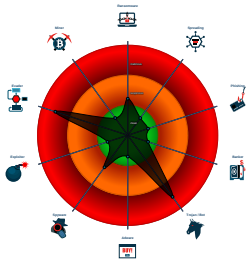
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- cpIaMuv3PV.exe (PID: 6364 cmdline: 'C:\Users\user\Desktop\cpIaMuv3PV.exe' MD5: A8911878F9C096C7BFE665B8076A8704)
  - schtasks.exe (PID: 6476 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OUCEGOEkZUvjuG' /XML 'C:\Users\user\AppData\Local\Temp\tmp2685.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6492 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cpIaMuv3PV.exe (PID: 6552 cmdline: C:\Users\user\Desktop\cpIaMuv3PV.exe MD5: A8911878F9C096C7BFE665B8076A8704)
- dhcpmon.exe (PID: 7060 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: A8911878F9C096C7BFE665B8076A8704)
  - schtasks.exe (PID: 6388 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OUCEGOEkZUvjuG' /XML 'C:\Users\user\AppData\Local\Temp\tmp7E79.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 976 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 6232 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: A8911878F9C096C7BFE665B8076A8704)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "6f656d69-7475-8807-1300-00",
  "Group": "worker",
  "Domain1": "",
  "Domain2": "hailongfvt.zapto.org",
  "Port": 3365,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.300425603.000000000331 1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.509285336.000000000519 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
00000004.00000002.509285336.000000000519 0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
00000004.00000002.508238274.000000000399 9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.508238274.000000000399 9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x2ef5:$a: NanoCore • 0x2f4e:$a: NanoCore • 0x2f8b:$a: NanoCore • 0x3004:$a: NanoCore • 0x166af:$a: NanoCore • 0x166c4:$a: NanoCore • 0x166f9:$a: NanoCore • 0x2f16b:$a: NanoCore • 0x2f180:$a: NanoCore • 0x2f1b5:$a: NanoCore • 0x2f57:$b: ClientPlugin • 0x2f94:$b: ClientPlugin • 0x3892:$b: ClientPlugin • 0x389f:$b: ClientPlugin • 0x1646b:$b: ClientPlugin • 0x16486:$b: ClientPlugin • 0x164b6:$b: ClientPlugin • 0x166cd:$b: ClientPlugin • 0x16702:$b: ClientPlugin • 0x2ef27:$b: ClientPlugin • 0x2ef42:$b: ClientPlugin

Click to see the 37 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.dhcpmon.exe.45b6850.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
8.2.dhcpmon.exe.45b6850.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
8.2.dhcpmon.exe.45b6850.3.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
8.2.dhcpmon.exe.45b6850.3.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xe0f5:$a: NanoCore • 0xe105:$a: NanoCore • 0xe339:$a: NanoCore • 0xe34d:$a: NanoCore • 0xe38d:$a: NanoCore • 0xe154:$b: ClientPlugin • 0xe356:$b: ClientPlugin • 0xe396:$b: ClientPlugin • 0xe27b:$c: ProjectData • 0xec82:$d: DESCrypto • 0x1664e:$e: KeepAlive • 0x1463c:$g: LogClientMessage • 0x10837:$i: get_Connected • 0xefb8:$j: #=q • 0xefe8:$j: #=q • 0xf004:$j: #=q • 0xf034:$j: #=q • 0xf050:$j: #=q • 0xf06c:$j: #=q • 0xf09c:$j: #=q • 0xf0b8:$j: #=q
4.2.cpIaMuv3PV.exe.5190000.7.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 69 entries				

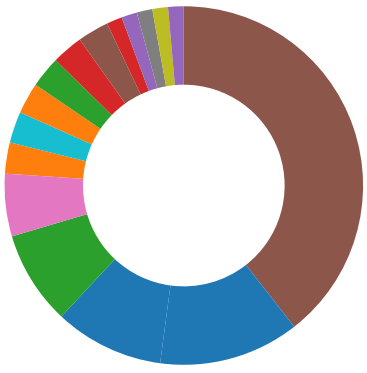
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

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 AntiVM_3

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

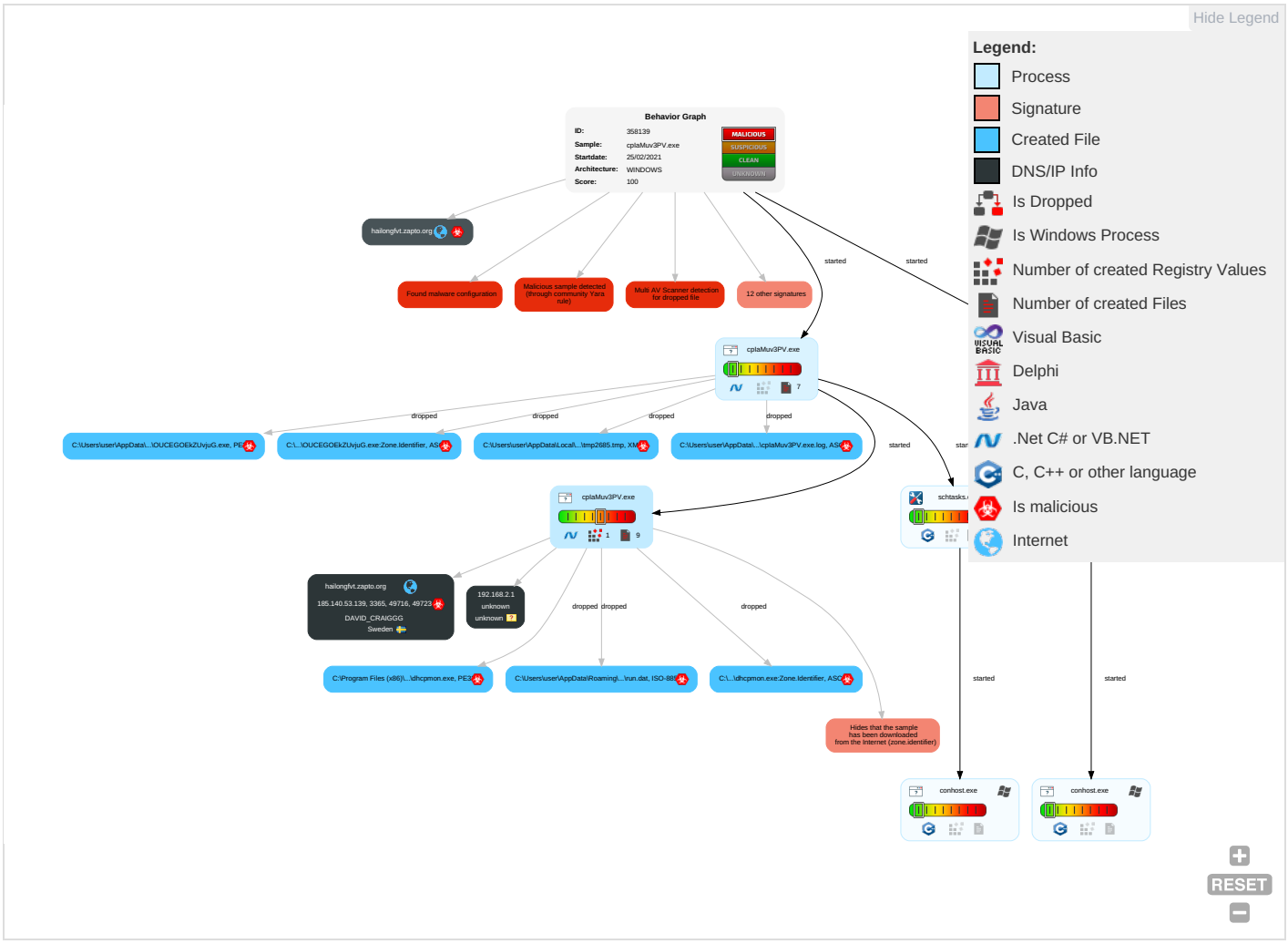
Detected Nanocore Rat

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	Security Software Discovery 2 1 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	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	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)	Disable or Modify Tools 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	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory 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	System Information Discovery 1 2	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 2	DCSync	Network Sniffing	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 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgra Insecure Protocols

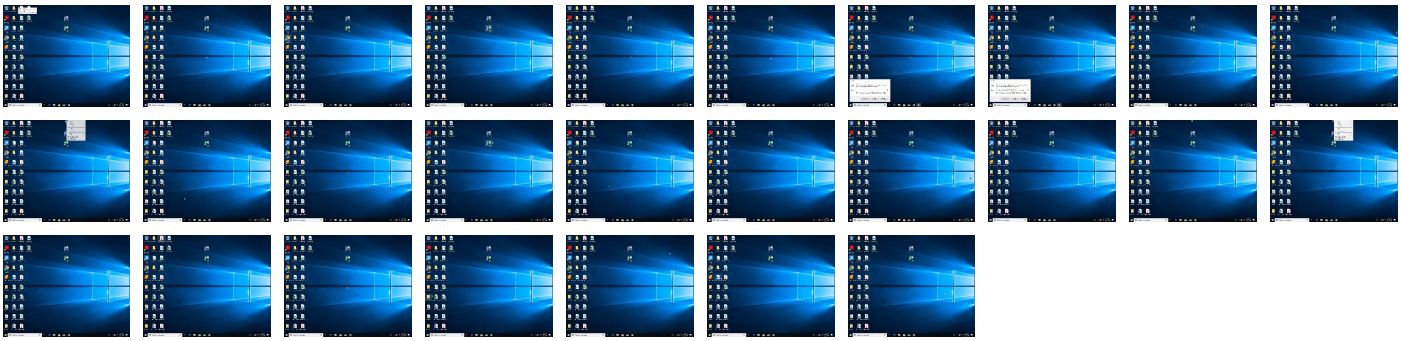
Behavior Graph



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
cplaMuv3PV.exe	31%	Virustotal		Browse
cplaMuv3PV.exe	19%	Metadefender		Browse
cplaMuv3PV.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
cplaMuv3PV.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	19%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe	19%	Metadefender		Browse
C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe	38%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.cplaMuv3PV.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.cpIaMuv3PV.exe.5270000.9.unpack	100%	Avira	TR/NanoCore.fadte		Download File
18.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	
http://tempuri.org/DS_Student_Fees.xsd	0%	Avira URL Cloud	safe	
http://tempuri.org/aLL_STUDENT_DATA.xsd	0%	Avira URL Cloud	safe	
http://tempuri.org/DS_Student_Fees.xsd;stbl_Student_Purchase_Details7DS_Student_Purchase_Detailsehtt	0%	Avira URL Cloud	safe	
http://tempuri.org/DS_All_Student_Bill.xsd;stbl_Product_Purchase_DetailsUhttp://tempuri.org/DS_Produ	0%	Avira URL Cloud	safe	
http://tempuri.org/DS_All_Student_Bill.xsd	0%	Avira URL Cloud	safe	
hailongfvt.zapto.org	0%	Avira URL Cloud	safe	
http://tempuri.org/DS_Stock.xsd	0%	Avira URL Cloud	safe	
http://tempuri.org/DS_Product_Purchase.xsd	0%	Avira URL Cloud	safe	
http://tempuri.org/DS_Student_Purchase_Details.xsd	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
hailongfvt.zapto.org	185.140.53.139	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
hailongfvt.zapto.org	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/DS_Student_Fees.xsd	dhcpmon.exe	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/aLL_STUDENT_DATA.xsd	dhcpmon.exe, dhcpmon.exe, 00000012.00000002.321328745.0000000000B52000.00000002.00020000.sdmp, cpIaMuv3PV.exe	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/DS_Student_Fees.xsd;stbl_Student_Purchase_Details7DS_Student_Purchase_Detailsehtt	cpIaMuv3PV.exe	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/DS_All_Student_Bill.xsd;stbl_Product_Purchase_DetailsUhttp://tempuri.org/DS_Produ	cpIaMuv3PV.exe	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	cpIaMuv3PV.exe, 00000000.00000002.247240720.0000000002F41000.00000004.00000001.sdmp, dhcpmon.exe, 00000008.00000002.300425603.0000000003311000.00000004.00000001.sdmp	false		high
http://tempuri.org/DS_All_Student_Bill.xsd	dhcpmon.exe	false	• Avira URL Cloud: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	cpIaMuv3PV.exe, 00000000.00000002.247240720.0000000002F41000.00000004.00000001.sdmp, dhcpmon.exe, 00000008.00000002.300425603.0000000003311000.00000004.00000001.sdmp	false		high
http://tempuri.org/DS_Stock.xsd	dhcpmon.exe, dhcpmon.exe, 00000012.00000002.321328745.0000000000B52000.00000002.00020000.sdmp, cpIaMuv3PV.exe	false	• Avira URL Cloud: safe	unknown
http://tempuri.org/DS_Product_Purchase.xsd	dhcpmon.exe	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://tempuri.org/DS_Student_Purchase_Details.xsd	dhcpmon.exe	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.140.53.139	unknown	Sweden		209623	DAVID_CRAIGGG	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358139
Start date:	25.02.2021
Start time:	04:01:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	cpIaMuv3PV.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:	32
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@12/9@23/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.8% (good quality ratio 1.4%) • Quality average: 61.1% • Quality standard deviation: 39.2%
HCA Information:	• Successful, ratio: 100% • 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 • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 51.103.5.159, 13.88.21.125, 204.79.197.200, 13.107.21.200, 51.11.168.160, 92.122.145.220, 104.43.193.48, 52.255.188.83, 23.218.208.56, 51.104.139.180, 2.20.142.209, 2.20.142.210, 93.184.221.240, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, vip1-par02p.wns.notify.trafficmanager.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, www.bing.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, client.wns.windows.com, fs.microsoft.com, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:02:18	API Interceptor	969x Sleep call for process: cpIaMuv3PV.exe modified
04:02:25	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
04:02:39	API Interceptor	1x Sleep call for process: dhcpmon.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.140.53.139	COMPANY PROFILE AND DOCUMENTED OFFER.exe	Get hash	malicious	Browse	
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	
	Quotation ATB-PR28500KINH.exe	Get hash	malicious	Browse	
	RFQ-BOHB-SS-FD6L4.exe	Get hash	malicious	Browse	
	PURCHASE_FABRICS_APPAREL_100%_COOTON.exe	Get hash	malicious	Browse	
	GT-082568-HSO-280820.DOCX.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
hailongfvt.zapto.org	COMPANY PROFILE AND DOCUMENTED OFFER.exe	Get hash	malicious	Browse	• 185.140.53.139

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DAVID_CRAIGGG	35dbds3GQG.exe	Get hash	malicious	Browse	• 185.140.53.138
	QXJGE2LOdP.exe	Get hash	malicious	Browse	• 185.140.53.138
	TxvR Order.exe	Get hash	malicious	Browse	• 185.140.53.43
	COMPANY PROFILE AND DOCUMENTED OFFER.exe	Get hash	malicious	Browse	• 185.140.53.139
	Attached file.exe	Get hash	malicious	Browse	• 185.244.30.113
	UNiOOhIN3e.exe	Get hash	malicious	Browse	• 185.244.30.241
	BzRmS2LLnB.exe	Get hash	malicious	Browse	• 91.193.75.94
	bDbA5Bf1k2.exe	Get hash	malicious	Browse	• 91.193.75.94
	SecuriteInfo.com.BehavesLike.Win32.Generic.dc.exe	Get hash	malicious	Browse	• 91.193.75.197
	Recibo del env#U00c3o.exe	Get hash	malicious	Browse	• 91.193.75.17
	Revised Order 193-002.doc	Get hash	malicious	Browse	• 91.193.75.197
	ynS1BQTyzO.exe	Get hash	malicious	Browse	• 91.193.75.252
	Quote RF-E79-STD-2021-087.xlsx	Get hash	malicious	Browse	• 91.193.75.252
	PO57891255564GYH11192643-2152021,pdf.exe	Get hash	malicious	Browse	• 185.140.53.136
	Attachment.exe	Get hash	malicious	Browse	• 185.244.30.113
	Query_Ref_CSQ5429996-dtd_0202102021-pdf.jar	Get hash	malicious	Browse	• 185.244.30.187
	Query_Ref_CSQ5429996-dtd_0202102021-pdf.jar	Get hash	malicious	Browse	• 185.244.30.187
	DHL_6368638172 receipt document,pdf.exe	Get hash	malicious	Browse	• 185.140.53.130
	47432000083600.xlsx	Get hash	malicious	Browse	• 185.244.30.21
	Belegbeleg DHL_119040, pdf.exe	Get hash	malicious	Browse	• 185.140.53.133

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\Desktop\cpIaMuv3PV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1272320
Entropy (8bit):	6.785801085900234
Encrypted:	false
SSDEEP:	12288:WeDlsV8+pn+BMQI6wUq0yGArEln20Em3ojpiOJ8UPm4wYHWW7xsbASBCt6e54qXo:ZLNgpRLrHz7xEBBCYe54qXAm3RBjA1
MD5:	A8911878F9C096C7BFE665B8076A8704
SHA1:	1DFFAAC5E83C62A0478095C68684BC4974F559DB
SHA-256:	498DF02F7263A2B524603CB58CD01C45115645F7586147FD39B19E930DFFC667
SHA-512:	B401F30A85FAB432401668863A34D63989BB6745D36331BA78EAAC5FCA16BA56E5212670CF2A596216A60BF329F642042B1BC8C4244998ABEE7319A7CA9ADD86
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 38%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5`.....P.....L.....:.. .....@.. ..... ..@.....p;..K....@...J..... ..... ..H.....text..... ..... ..`.rsrc....J...@...J.....@..@.rel oc.....h.....@..B.....;.....H.....?.....O.....0..#.....+.&...(....(.....(.....o.....*.....0.....+.&..8.....8.....+p..aa.+...na. ..mXE.....K...X....g(.....+.....&...+...eXE..... .../...>...M...h...q...z.....+..m(.....+.8~.....8u.....(.....8f.....(.....8W.....(.....8H.....(....+.(....82.....8-.....8$.....8..... 8.....&+..8.....8....*.0.....+.&...+8..ga.+...aa8x.....hY+D...+...gXE

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\cpIaMuv3PV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
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:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cpIaMuv3PV.exe.log	
Process:	C:\Users\user\Desktop\cpIaMuv3PV.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4sH:MgvjHK5HKXE1qHbHK5AHKzvRYHKhQnoR
MD5:	CB0A771DADBDC62238A0AB0D40CC3382
SHA1:	38A48365315A474D6E7117AC72A354935052051C
SHA-256:	BBB2C37AFB091B8A3E18FC1D8B2A35707D0B64B373CDBA5A147BBAAEABD24C2E
SHA-512:	6518C09AECF15B58D74B9E09A911ADB17CCB43B1508BEBAEEA9C1B563B766FBDA6B585E149AB16793DD2AD8761F7F6D68A18724369CF47FA023839C74F5549 0
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..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.Co

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):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4bE4K5AE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4sH:MgvjHK5HKXE1qHbHK5AHKzvRYHKhQnoR
MD5:	CB0A771DADBDC62238A0AB0D40CC3382
SHA1:	38A48365315A474D6E7117AC72A354935052051C
SHA-256:	BBB2C37AFB091B8A3E18FC1D8B2A35707D0B64B373CDBA5A147BBAAEABD24C2E
SHA-512:	6518C09AECF15B58D74B9E09A911ADB17CCB43B1508BEBAEEA9C1B563B766FBDA6B585E149AB16793DD2AD8761F7F6D68A18724369CF47FA023839C74F5549 0
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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..2,"System.Data, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..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.Co

C:\Users\user\AppData\Local\Temp\tmp2685.tmp	
Process:	C:\Users\user\Desktop\cpIaMuv3PV.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1663
Entropy (8bit):	5.186428793191548
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBAYtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3ue
MD5:	3C48812341687AA2F8C0ABD00611CCF8
SHA1:	5BF2AECFA0748C282DD2AC5A8AFF35622EB8C6C7
SHA-256:	B3BFE0ED81C4107CEC70B9503371D2F6E013BA046018E7A912F825F25EF45804
SHA-512:	06AD1F5C6D296A0D37368B3811488BF4D1220137D134AFD22C85D9230DCD8DA6F621BA52A3AEE0C953793A9507837257E2329DAEE2469A093ABA076B080A5D7
Malicious:	**true**
Reputation:	low
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>.. <StartWhenAv

C:\Users\user\AppData\Local\Temp\tmp7E79.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1663
Entropy (8bit):	5.186428793191548
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/dp7hdMlNMFpdU/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBAYtn:cbhH7MlNQ8/rydbz9I3YODOLNdq3ue
MD5:	3C48812341687AA2F8C0ABD00611CCF8
SHA1:	5BF2AECFA0748C282DD2AC5A8AFF35622EB8C6C7
SHA-256:	B3BFE0ED81C4107CEC70B9503371D2F6E013BA046018E7A912F825F25EF45804
SHA-512:	06AD1F5C6D296A0D37368B3811488BF4D1220137D134AFD22C85D9230DCD8DA6F621BA52A3AEE0C953793A9507837257E2329DAEE2469A093ABA076B080A5D7
Malicious:	false
Reputation:	low
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>.. <StartWhenAv

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\cpIaMuv3PV.exe
File Type:	ISO-8859 text, with NEL line terminators

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:sst:sst
MD5:	5A86F30FF0CEF5D88164B253F6B691F1
SHA1:	CFC30B4C368FAF9CECD6158AD98921760783FA49
SHA-256:	26C1FDB652FA78AD690EA97E65C2C318D76438BA3D69D896001422D7D47F7DB9
SHA-512:	1205329F6FBEB6B6E07E698F69438C9B7B264FFE61B8946F2C0856C8194AB274B20E89DE772D302B80ED36B43E3D1F30341E950372F7B4D6FB03A9A6E20D13C8
Malicious:	**true**
Reputation:	low
Preview:	Q..6...H

C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe	
Process:	C:\Users\user\Desktop\cpIaMuv3PV.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1272320
Entropy (8bit):	6.785801085900234
Encrypted:	false
SSDEEP:	12288:WeDlsV8+pn+BMQI6wUq0yGArEln20Em3ojpiOJ8UPm4wYHWW7xsbASBCt6e54qXo:ZLNgpRLrHz7xEBBCYe54qXAm3RBjA1
MD5:	A8911878F9C096C7BFE665B8076A8704
SHA1:	1DFFAAC5E83C62A0478095C68684BC4974F559DB
SHA-256:	498DF02F7263A2B524603CB58CD01C45115645F7586147FD39B19E930DFFC667
SHA-512:	B401F30A85FAB432401668863A34D63989BB6745D36331BA78EAAC5FCA16BA56E5212670CF2A596216A60BF329F642042B1BC8C4244998ABEE7319A7CA9ADD86
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 19%, Browse • Antivirus: ReversingLabs, Detection: 38%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5`.....P.....L.....;... .....@.. ..... ..@.....p;..K....@...J..... ..... ..H.....text..... ..... ..`.rsrc....J...@...J.....@..@.rel oc.....h.....@..B.....;.....H.....?.....O.....0..#.....+.&...(....(.....(....o....*.....0.....+.&..8.....8.....+p..aa.+...na. ..mXE.....K...X....g(.....+.....&...+...eXE..... .../...>...M...h...q...z.....+..m(.....+.8~.....8u.....(.....8f.....(.....8W.....(.....8H.....(....+.(....82.....8-.....8$.....8..... 8.....&+..8.....8....*.0.....+.&...+8..ga.+...aa8x.....hY+D...+...gXE

C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\cpIaMuv3PV.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**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.785801085900234

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	cpIaMuv3PV.exe
File size:	1272320
MD5:	a8911878f9c096c7bfe665b8076a8704
SHA1:	1dffaac5e83c62a0478095c68684bc4974f559db
SHA256:	498df02f7263a2b524603cb58cd01c45115645f7586147fd39b19e930dffc667
SHA512:	b401f30a85fab432401668863a34d63989bb6745d36331a78eaac5fca16ba56e5212670cf2a596216a60bf329f642042b1bc8c4244998abee7319a7ca9add86
SSDEEP:	12288:WeDlsV8+pn+BMQl6wUq0yGArEln20Em3ojpiOJ8UPm4wYHWW7xsbASBCt6e54qXo:ZLNgpRLrHz7xEBBCYe54qXAm3RBjA1
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....5`.....P.....L.....;... .....@.. .....@.....

File Icon

Icon Hash:	c870f0f0d8fc7c03

Static PE Info

General

Entrypoint:	0x533bbe
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:	0x6035C6C3 [Wed Feb 24 03:23:47 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

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x133b70	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x134000	0x4a00	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x13a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x131bc4	0x131c00	False	0.531282738399	data	6.81640542834	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x134000	0x4a00	0x4a00	False	0.273807010135	data	3.78141625052	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x13a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x134100	0x4228	dBase III DBT, version number 0, next free block index 40		
RT_GROUP_ICON	0x138338	0x14	data		
RT_VERSION	0x13835c	0x366	data		
RT_MANIFEST	0x1386d4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

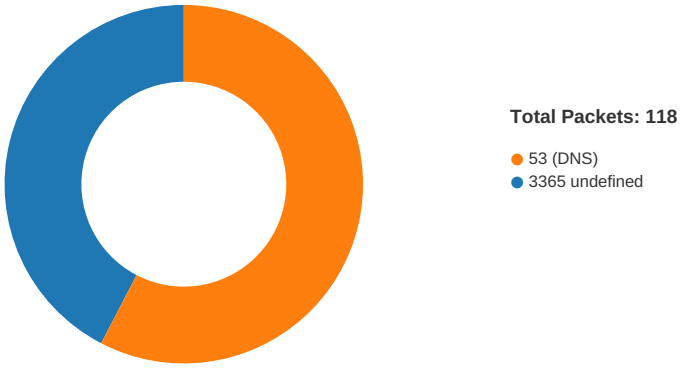
DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright D S Damat Online
Assembly Version	1.1.8.14
InternalName	MdConstant.exe
FileVersion	1.1.8.14
CompanyName	D S Damat Online
LegalTrademarks	
Comments	
ProductName	D'S Damat
ProductVersion	1.1.8.14
FileDescription	D'S Damat
OriginalFilename	MdConstant.exe

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 04:02:26.473370075 CET	49716	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:26.518624067 CET	3365	49716	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:27.120229959 CET	49716	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:27.165539980 CET	3365	49716	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:27.823421001 CET	49716	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:27.868802071 CET	3365	49716	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:33.288084030 CET	49723	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:33.335201025 CET	3365	49723	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:33.964596033 CET	49723	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:34.009816885 CET	3365	49723	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:34.574018955 CET	49723	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:34.620681047 CET	3365	49723	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:38.758946896 CET	49730	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:38.803987026 CET	3365	49730	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:39.464996099 CET	49730	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:39.511528969 CET	3365	49730	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:40.074441910 CET	49730	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:40.120079041 CET	3365	49730	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:44.696266890 CET	49732	3365	192.168.2.7	185.140.53.139

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 04:02:44.741364956 CET	3365	49732	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:45.278019905 CET	49732	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:45.323188066 CET	3365	49732	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:45.966013908 CET	49732	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:46.011109114 CET	3365	49732	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:50.501729965 CET	49733	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:50.546786070 CET	3365	49733	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:51.122309923 CET	49733	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:51.167396069 CET	3365	49733	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:51.825455904 CET	49733	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:51.870436907 CET	3365	49733	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:56.027457952 CET	49736	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:56.074837923 CET	3365	49736	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:56.622755051 CET	49736	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:56.667952061 CET	3365	49736	185.140.53.139	192.168.2.7
Feb 25, 2021 04:02:57.326021910 CET	49736	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:02:57.371155977 CET	3365	49736	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:01.943954945 CET	49737	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:01.989780903 CET	3365	49737	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:02.498291969 CET	49737	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:02.543540001 CET	3365	49737	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:03.045150042 CET	49737	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:03.090298891 CET	3365	49737	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:07.180772066 CET	49744	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:07.225883007 CET	3365	49744	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:07.733062029 CET	49744	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:07.780318022 CET	3365	49744	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:08.295571089 CET	49744	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:08.340837955 CET	3365	49744	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:12.445955038 CET	49745	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:12.491339922 CET	3365	49745	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:13.092895031 CET	49745	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:13.138628960 CET	3365	49745	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:13.796041012 CET	49745	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:13.841634035 CET	3365	49745	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:17.944457054 CET	49751	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:17.989474058 CET	3365	49751	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:18.586312056 CET	49751	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:18.631408930 CET	3365	49751	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:19.187109947 CET	49751	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:19.234419107 CET	3365	49751	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:23.361229897 CET	49752	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:23.406435013 CET	3365	49752	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:24.094458103 CET	49752	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:24.139643908 CET	3365	49752	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:24.703216076 CET	49752	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:24.748512030 CET	3365	49752	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:29.927272081 CET	49753	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:29.973731995 CET	3365	49753	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:30.578682899 CET	49753	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:30.623743057 CET	3365	49753	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:31.284149885 CET	49753	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:31.329207897 CET	3365	49753	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:35.457288027 CET	49754	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:35.502422094 CET	3365	49754	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:36.079209089 CET	49754	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:36.126812935 CET	3365	49754	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:36.782363892 CET	49754	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:36.829159975 CET	3365	49754	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:40.945180893 CET	49760	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:40.990593910 CET	3365	49760	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:41.501486063 CET	49760	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:41.546868086 CET	3365	49760	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:42.048398972 CET	49760	3365	192.168.2.7	185.140.53.139

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 04:03:42.093969107 CET	3365	49760	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:46.222960949 CET	49767	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:46.268110991 CET	3365	49767	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:46.767564058 CET	49767	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:46.813080072 CET	3365	49767	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:47.330116034 CET	49767	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:47.376920938 CET	3365	49767	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:51.506802082 CET	49768	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:51.554889917 CET	3365	49768	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:52.065949917 CET	49768	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:52.111140013 CET	3365	49768	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:52.611891985 CET	49768	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:52.657094955 CET	3365	49768	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:56.751504898 CET	49769	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:56.796696901 CET	3365	49769	185.140.53.139	192.168.2.7
Feb 25, 2021 04:03:57.299932003 CET	49769	3365	192.168.2.7	185.140.53.139
Feb 25, 2021 04:03:57.344906092 CET	3365	49769	185.140.53.139	192.168.2.7

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 04:02:08.444654942 CET	61242	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:08.465351105 CET	58562	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:08.511763096 CET	53	61242	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:08.522351980 CET	53	58562	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:08.842672110 CET	56590	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:08.901761055 CET	53	56590	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:08.909348965 CET	60501	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:08.960756063 CET	53	60501	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:09.798820972 CET	53775	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:09.861493111 CET	53	53775	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:11.026640892 CET	51837	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:11.088948011 CET	53	51837	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:12.339931965 CET	55411	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:12.388650894 CET	53	55411	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:13.068850040 CET	63668	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:13.165524006 CET	53	63668	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:13.600414991 CET	54640	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:13.649146080 CET	53	54640	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:14.637718916 CET	58739	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:14.686374903 CET	53	58739	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:15.707830906 CET	60338	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:15.756501913 CET	53	60338	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:16.648066998 CET	58717	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:16.701535940 CET	53	58717	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:17.861438036 CET	59762	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:17.920944929 CET	53	59762	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:19.219341993 CET	54329	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:19.270757914 CET	53	54329	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:20.650923967 CET	58052	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:20.708071947 CET	53	58052	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:25.123212099 CET	54008	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:25.171848059 CET	53	54008	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:26.390512943 CET	59451	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:26.452054977 CET	53	59451	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:26.535105944 CET	52914	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:26.586486101 CET	53	52914	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:27.798062086 CET	64569	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:27.846755981 CET	53	64569	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:28.979156017 CET	52816	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:29.027985096 CET	53	52816	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:30.647952080 CET	50781	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:30.696743965 CET	53	50781	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:33.225302935 CET	54230	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 04:02:33.286288023 CET	53	54230	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:33.478563070 CET	54911	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:33.535832882 CET	49958	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:33.542650938 CET	53	54911	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:33.584554911 CET	53	49958	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:34.656936884 CET	50860	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:34.708436966 CET	53	50860	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:35.782387018 CET	50452	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:35.841712952 CET	53	50452	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:37.101480961 CET	59730	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:37.159876108 CET	53	59730	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:38.307773113 CET	59310	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:38.359249115 CET	53	59310	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:38.668920040 CET	51919	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:38.728554010 CET	53	51919	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:40.096520901 CET	64296	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:40.156225920 CET	53	64296	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:44.633652925 CET	56680	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:44.694955111 CET	53	56680	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:50.443129063 CET	58820	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:50.500276089 CET	53	58820	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:52.572180986 CET	60983	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:52.622535944 CET	53	60983	8.8.8.8	192.168.2.7
Feb 25, 2021 04:02:55.967534065 CET	49247	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:02:56.026488066 CET	53	49247	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:01.889230967 CET	52286	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:01.942831039 CET	53	52286	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:03.192819118 CET	56064	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:03.260288000 CET	53	56064	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:03.364636898 CET	63744	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:03.424544096 CET	53	63744	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:04.012682915 CET	61457	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:04.074146032 CET	53	61457	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:06.568280935 CET	58367	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:06.622641087 CET	53	58367	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:07.117599964 CET	60599	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:07.179799080 CET	53	60599	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:12.384613991 CET	59571	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:12.444648027 CET	53	59571	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:16.889359951 CET	52689	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:16.946671963 CET	53	52689	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:17.883157015 CET	50290	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:17.943077087 CET	53	50290	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:23.301930904 CET	60427	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:23.359168053 CET	53	60427	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:29.730482101 CET	56209	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:29.791511059 CET	53	56209	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:35.393599033 CET	59582	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:35.455698013 CET	53	59582	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:38.899404049 CET	60949	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:38.948132992 CET	53	60949	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:39.571975946 CET	58542	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:39.640474081 CET	53	58542	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:39.889245987 CET	59179	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:39.963926077 CET	53	59179	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:40.236311913 CET	60927	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:40.293179035 CET	53	60927	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:40.766766071 CET	57854	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:40.823815107 CET	53	57854	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:40.886550903 CET	62026	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:40.943595886 CET	53	62026	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:41.343502045 CET	59453	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:41.392199993 CET	53	59453	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:41.951112032 CET	62468	53	192.168.2.7	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 04:03:42.010968924 CET	53	62468	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:42.612159014 CET	52563	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:42.664016008 CET	53	52563	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:43.485431910 CET	54721	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:43.545458078 CET	53	54721	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:44.444976091 CET	62826	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:44.496613026 CET	53	62826	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:45.043754101 CET	62046	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:45.100975037 CET	53	62046	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:46.162457943 CET	51223	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:46.219542980 CET	53	51223	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:51.447653055 CET	63908	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:51.504779100 CET	53	63908	8.8.8.8	192.168.2.7
Feb 25, 2021 04:03:56.687129021 CET	49226	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:03:56.749474049 CET	53	49226	8.8.8.8	192.168.2.7
Feb 25, 2021 04:04:01.934845924 CET	60212	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:04:01.995347977 CET	53	60212	8.8.8.8	192.168.2.7
Feb 25, 2021 04:04:07.202697992 CET	58867	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:04:07.262625933 CET	53	58867	8.8.8.8	192.168.2.7
Feb 25, 2021 04:04:09.710293055 CET	50864	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:04:09.758932114 CET	53	50864	8.8.8.8	192.168.2.7
Feb 25, 2021 04:04:12.467452049 CET	61504	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:04:12.527344942 CET	53	61504	8.8.8.8	192.168.2.7
Feb 25, 2021 04:04:17.715581894 CET	60231	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:04:17.781374931 CET	53	60231	8.8.8.8	192.168.2.7
Feb 25, 2021 04:04:22.932643890 CET	50095	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:04:22.994004011 CET	53	50095	8.8.8.8	192.168.2.7
Feb 25, 2021 04:04:28.178107023 CET	59654	53	192.168.2.7	8.8.8.8
Feb 25, 2021 04:04:28.235445976 CET	53	59654	8.8.8.8	192.168.2.7

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 04:02:26.390512943 CET	192.168.2.7	8.8.8.8	0xed11	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:33.225302935 CET	192.168.2.7	8.8.8.8	0xbae1	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:38.668920040 CET	192.168.2.7	8.8.8.8	0x12e8	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:44.633652925 CET	192.168.2.7	8.8.8.8	0x6a05	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:50.443129063 CET	192.168.2.7	8.8.8.8	0xd3d0	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:55.967534065 CET	192.168.2.7	8.8.8.8	0x179a	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:01.889230967 CET	192.168.2.7	8.8.8.8	0x68b5	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:07.117599964 CET	192.168.2.7	8.8.8.8	0x2214	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:12.384613991 CET	192.168.2.7	8.8.8.8	0xef78	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:17.883157015 CET	192.168.2.7	8.8.8.8	0x63c2	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:23.301930904 CET	192.168.2.7	8.8.8.8	0x4ab5	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:29.730482101 CET	192.168.2.7	8.8.8.8	0x7ae5	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:35.393599033 CET	192.168.2.7	8.8.8.8	0x3d6e	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:40.886550903 CET	192.168.2.7	8.8.8.8	0x30dd	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:46.162457943 CET	192.168.2.7	8.8.8.8	0x47c8	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:51.447653055 CET	192.168.2.7	8.8.8.8	0x1e58	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:56.687129021 CET	192.168.2.7	8.8.8.8	0x535	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:01.934845924 CET	192.168.2.7	8.8.8.8	0x524a	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 04:04:07.202697992 CET	192.168.2.7	8.8.8.8	0xedd9	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:12.467452049 CET	192.168.2.7	8.8.8.8	0x6a27	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:17.715581894 CET	192.168.2.7	8.8.8.8	0x76b0	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:22.932643890 CET	192.168.2.7	8.8.8.8	0x731a	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:28.178107023 CET	192.168.2.7	8.8.8.8	0xfe23	Standard query (0)	hailongfvt .zapto.org	A (IP address)	IN (0x0001)

DNS Answers

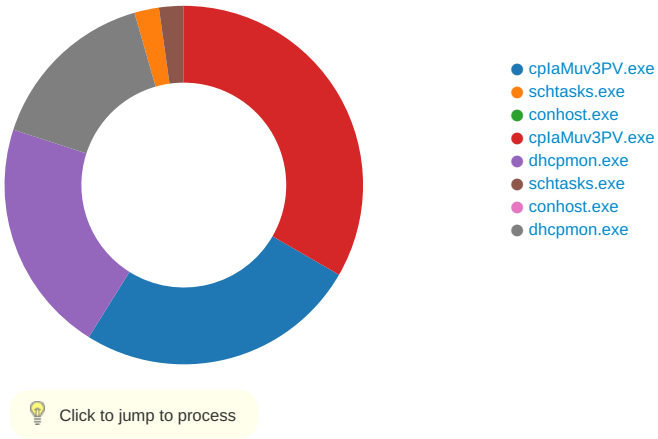
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 04:02:26.452054977 CET	8.8.8.8	192.168.2.7	0xed11	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:33.286288023 CET	8.8.8.8	192.168.2.7	0xbae1	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:38.728554010 CET	8.8.8.8	192.168.2.7	0x12e8	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:44.694955111 CET	8.8.8.8	192.168.2.7	0x6a05	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:50.500276089 CET	8.8.8.8	192.168.2.7	0xd3d0	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:02:56.026488066 CET	8.8.8.8	192.168.2.7	0x179a	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:01.942831039 CET	8.8.8.8	192.168.2.7	0x68b5	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:07.179799080 CET	8.8.8.8	192.168.2.7	0x2214	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:12.444648027 CET	8.8.8.8	192.168.2.7	0xef78	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:17.943077087 CET	8.8.8.8	192.168.2.7	0x63c2	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:23.359168053 CET	8.8.8.8	192.168.2.7	0x4ab5	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:29.791511059 CET	8.8.8.8	192.168.2.7	0x7ae5	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:35.455698013 CET	8.8.8.8	192.168.2.7	0x3d6e	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:40.943595886 CET	8.8.8.8	192.168.2.7	0x30dd	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:46.219542980 CET	8.8.8.8	192.168.2.7	0x47c8	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:51.504779100 CET	8.8.8.8	192.168.2.7	0x1e58	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:03:56.749474049 CET	8.8.8.8	192.168.2.7	0x535	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:01.995347977 CET	8.8.8.8	192.168.2.7	0x524a	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:07.262625933 CET	8.8.8.8	192.168.2.7	0xedd9	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:12.527344942 CET	8.8.8.8	192.168.2.7	0x6a27	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:17.781374931 CET	8.8.8.8	192.168.2.7	0x76b0	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 04:04:22.994004011 CET	8.8.8.8	192.168.2.7	0x731a	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)
Feb 25, 2021 04:04:28.235445976 CET	8.8.8.8	192.168.2.7	0xfe23	No error (0)	hailongfvt .zapto.org		185.140.53.139	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: cplaMuv3PV.exe PID: 6364 Parent PID: 5680

General

Start time:	04:02:15
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\cplaMuv3PV.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\cplaMuv3PV.exe'
Imagebase:	0xb30000
File size:	1272320 bytes
MD5 hash:	A8911878F9C096C7BFE665B8076A8704
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: 00000000.00000002.247716186.0000000003FCD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.247716186.0000000003FCD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.247716186.0000000003FCD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.247240720.0000000002F41000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.248243542.00000000040F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.248243542.00000000040F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.248243542.00000000040F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.247304436.0000000002FBC000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5CCF06	unknown
C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C41DD66	CopyFileW
C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C41DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2685.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C417038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cpIaMuv3PV.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2685.tmp	success or wait	1	6C416A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c3 c6 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 1c 13 00 00 4c 00 00 00 00 00 00 be 3b 13 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 13 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....5`.......... ....P......L.......;... ....@.. ....@................	success or wait	5	6C41DD66	CopyFileW
C:\Users\user\AppData\Roaming\OUCEGOEkZUvjuG.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C41DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp2685.tmp	unknown	1663	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microso ft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registrati	success or wait	1	6C411B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\cpIaMuv3PV.exe.log	unknown	1400	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D8DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C411B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C411B4F	ReadFile

Analysis Process: schtasks.exe PID: 6476 Parent PID: 6364

General

Start time:	04:02:20
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OUCEGOEkZUvjuG' /XML 'C:\Users\user\AppData\Local\Temp\tmp2685.tmp'
Imagebase:	0x2b0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp2685.tmp	unknown	2	success or wait	1	2BAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp2685.tmp	unknown	1664	success or wait	1	2BABD9	ReadFile

Analysis Process: conhost.exe PID: 6492 Parent PID: 6476

General

Start time:	04:02:21
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: cpIaMuv3PV.exe PID: 6552 Parent PID: 6364

General

Start time:	04:02:22
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\cpIaMuv3PV.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\cpIaMuv3PV.exe
Imagebase:	0x4b0000
File size:	1272320 bytes
MD5 hash:	A8911878F9C096C7BFE665B8076A8704
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: 00000004.00000002.509285336.0000000005190000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.509285336.0000000005190000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.508238274.0000000003999000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.508238274.0000000003999000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.501066810.0000000002951000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.509339734.0000000005270000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.509339734.0000000005270000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.509339734.0000000005270000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.498104256.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.498104256.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.498104256.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5CCF06	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C41BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	6C411E60	CreateFileW
C:\Program Files (x86)\DHCP Monitor	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C41BEFF	CreateDirectoryW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C41DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C41DD66	CopyFileW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C41BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C41BEFF	CreateDirectoryW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\cplaMuv3PV.exe:Zone.Identifier	success or wait	1	6C392935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	51 c2 dd 36 85 d9 d8 48	Q..6...H	success or wait	1	6C411B4F	WriteFile
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 c3 c6 35 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 1c 13 00 00 4c 00 00 00 00 00 00 be 3b 13 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 13 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L.....5`.......... ....P......L.......;... ....@.. ....@................	success or wait	5	6C41DD66	CopyFileW
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6C41DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5003DE	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C411B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C411B4F	ReadFile
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	6D58D72F	unknown
C:\Windows\Microsoft.NET\assembly\GAC_32\mscorlib\v4.0_4.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	6D58D72F	unknown
C:\Users\user\Desktop\cpIaMuv3PV.exe	unknown	4096	success or wait	1	6D58D72F	unknown
C:\Users\user\Desktop\cpIaMuv3PV.exe	unknown	512	success or wait	1	6D58D72F	unknown

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run	DHCP Monitor	unicode	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	success or wait	1	6C41646A	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 7060 Parent PID: 3292

General

Start time:	04:02:34
Start date:	25/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0x7ff6e70f0000
File size:	1272320 bytes
MD5 hash:	A8911878F9C096C7BFE665B8076A8704
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: 00000008.00000002.300425603.0000000003311000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000008.00000002.302116757.0000000004318000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.302116757.0000000004318000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.302116757.0000000004318000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000008.00000002.300490631.0000000003359000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 19%, Metadefender, Browse • Detection: 38%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5CCF06	unknown
C:\Users\user\AppData\Local\Temp\tmp7E79.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6C417038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6D8DC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7E79.tmp	success or wait	1	6C416A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7E79.tmp	unknown	1663	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 66 72 6f 6e 74 64 65 73 6b 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69	<?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>..</Registrati	success or wait	1	6C411B4F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\dhcpmon.exe.log	unknown	1400	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6D8DC907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C411B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C411B4F	ReadFile

Analysis Process: schtasks.exe PID: 6388 Parent PID: 7060

General

Start time:	04:02:43
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\OUCEGOEkZUvjuG' /XML 'C:\Users\user\AppData\Local\Temp\tmp7E79.tmp'
Imagebase:	0x1070000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04

Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp7E79.tmp	unknown	2	success or wait	1	107AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp7E79.tmp	unknown	1664	success or wait	1	107ABD9	ReadFile

Analysis Process: conhost.exe PID: 976 Parent PID: 6388

General

Start time:	04:02:44
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff774ee0000
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: 6232 Parent PID: 7060

General

Start time:	04:02:45
Start date:	25/02/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xb50000
File size:	1272320 bytes
MD5 hash:	A8911878F9C096C7BFE665B8076A8704
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: 00000012.00000002.322544364.00000000042C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.322544364.00000000042C9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.322397159.00000000032C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.322397159.00000000032C1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000012.00000002.321286560.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.321286560.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.321286560.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5CCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D5CCF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D5A5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5ACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D5003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D5003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D5A5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C411B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C411B4F	ReadFile

Disassembly

Code Analysis