ID: 382764
Sample Name: Invoice PaymentPDF.vbs
Cookbook: default.jbs
Time: 16:31:09
Date: 06/04/2021
Version: 31.0.0 Emerald

Table of Contents

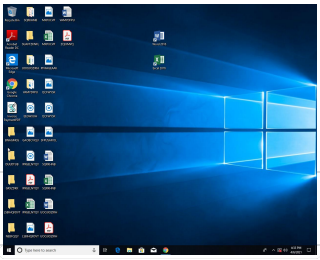
Analysis Report Invoice PaymentPDF.vbs

Overview

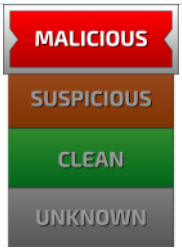
General Information

Sample Name:	Invoice PaymentPDF.vbs
Analysis ID:	382764
MD5:	3911ee0964b7aa..
SHA1:	b6f21d1f4a6f332...
SHA256:	ea5784a4389f86b.
Tags:	NanoCore RAT vbs
Infos:	

Most interesting Screenshot:



Detection



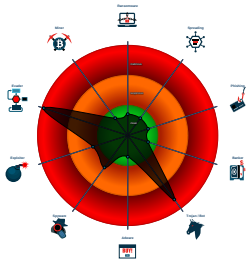
Nanocore AsyncRAT

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

Signatures

- Antivirus detection for dropped file
- Benign windows process drops PE f...
- Detected Nanocore Rat
- Detected unpacking (overwrites its o...
- Found malware configuration
- Malicious sample detected (through ...
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e....
- VBScript performs obfuscated calls ...
- Yara detected AsyncRAT
- Yara detected Nanocore RAT
- .NET source code contains potentia...

Classification



Startup

- **System is w10x64**
- wscript.exe (PID: 5648 cmdline: C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Invoice PaymentPDF.vbs' MD5: 9A68ADD12EB50DDE7586782C3EB9FF9C)
  - file.exe (PID: 360 cmdline: 'C:\Users\user~1\AppData\Local\Temp\file.exe' MD5: 76D2BB0F57BBF02E190055FCDB3663DB)
  - name.exe (PID: 4704 cmdline: 'C:\Users\user~1\AppData\Local\Temp\name.exe' MD5: 50B53CECA7021AD9ABEA4074A634680A)
- **cleanup**

Malware Configuration

Threatname: AsyncRAT

```
{
  "Server": "23.238.217.173",
  "Ports": "6606,7707,8808",
  "Version": "0.5.7B",
  "Autorun": "false",
  "Install_Folder": "%AppData%",
  "Install_File": "",
  "AES_key": "rCdLgrV42q0DuDQzYbk2auSrJRoHXPHS",
  "Mutex": "AsyncMutex_6SI8OkPnk",
  "AntiDetection": "false",
  "External_config_on_Pastebin": "null",
  "BDOS": "false",
  "Startup_Delay": "3",
  "HWID": "null",
  "Certificate":
"MIIE8jCCAtqgAwIBAgIQAJkhHU+BH915hv7LViGwzzANBgkqhkiG9w0BAQ0FADAaMRgwFgYDVQQDDA9Bc3luY1JBVCBTZXJ2ZXIwIBcNMjAxMTA3MTkxMTE5WhgPOTk5OTEyMzEyMzU5NTlaMBoxGDAWBgNVBAMMD0FzeW5jUkFUIFNlcnZlcjCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJ2Kr4dwEtG7paj+p7bT61qNpAHg0vCScR1TFYJ9AFuPQMEPGEaB7gCf40qGTli8A/ac0EI2vXm8+pKrmu2ae50KltRwInh3rlKQOV3s6p1sGE7cZNc0a8+YjbLtvex6jx7mc+RrPNDX7ztZb5yFXDOxOmXNhcisF7GQLeIXdRp3AzEafDoS0S6N5AJlUCyI3/vHk6FbI8GZtjjj2fvYQKeX/oQyv+KDwx3m7BO6NTaLVCrDBikJZpoajcvmctTlR5u5HgtzIQ6QfZtt3SMPOC7vE4QOwfIS5Y5EJ2H8u5qJ3f7aomyxDUSV8snsvDpXg5Nk6WAOf0Lh10sjWM82Q8wCvaeijVkYMVTJYZXFhkc7C0+c6+19GVNvJlWdbSTeZKCOwCJD2TEiqJfCpeaySqJpvAqMhUj1qL+hX9SNS5uC32FcxVWve/COS1s6piR4GO5GWqErJp5dKDNyxnJWW27pyivcuciKSfj7g4ObXA3ABARzJucyyAV2rAn9N18JwOguGAu3boSDtgvIUYiUAupPK0a7Lf8E+eiLWMsVdX5uXRy2M5Lw/VGJ9EiMbswzfJN0SWV5kp1QESUzkIZWMBKmfFJ3JgipR/mSxBXT6+7FQfLWEil3T/1UKE9Rm7Q4k0kcYX/SpzUvgZadwyaI8hbjz3uiaFV9/FSFPrq6qPkxAgMBAAGjMjAwMB0GA1UdDgQWBBTIOzfxNrixzR4oMI+dIEjFy3dMfTAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBDQUAA4ICAQBp13OHOR30C2YvzChrPHZIxlXZWnFJz5nazJy2kvFXCoq+ENu1aTJtpwN0XR0FhLyBhbWDTqoxoxJK33bfPjSn2Vrr44Anpdfjn+wBGfvic8btWTlPE/0g0vYDlv3OmIibf0s7ob/fVNaFiBumJZiPKguGya283ycWRF28JN/mqV7A6r4Py26CtTaGAs36Kzg5hgAxRoXjEMl8PzbYFjRFzteO0OA2Y9p2wp79W+h9JY0rGW/UTQqvUNpV2KfdKf5eGOKv5PHhzcQ56L+RydGaO0BL0WAcy/wvu/rW6+XPDhotNcVbsFGxPdMXUGfbzT5+4ugJv9n95fn3f6EWVitDdt/b1iz55VkbpbHr3YaPT/LVp9qXSHgg0lz9FQsdkssrD2Ete5NdlTOezia4jvxgkb2vdYIWNSURnNJXmH6CPVnrRa4juhjKtXsG0dOdxz5PSRJYmukFy8gl283yeOmDEqSDo9rQ9ywxtcL2IJYHzkmo6vctWnQnUaD8H87zz1YN3f1FbQEXovEDkIB7AiyRG2kfeRNMbEFCd0u1TXajD4z/+4+EGAGYpU7Laqar0PbFAuBe8/SAPfAsYqLdQ5TKIm8f54miRP72ySJ7+4kus25+19LdQmUJM79EKeFw2R6COJRRTvZ4hP3xqwn4yPULDJbU+CBSV9QY1YwU4ziUCQ==",
  "ServerSignature":
"b7cZ72qbdlFxoVfpO/0tHE5xKg0vNw58XJ+PsP/eWucYIkdeP6fnlIwnxnXsvoEWxw3CuGFtcGjY9btemVUwPNMNu2wCsW4Plb9qpUk7TXu6kX0D+z5illmf1+q1/535hHDE0vGVhjFy7mX+LHrPyDC4o+zRjsy970eMY24er5ru4bN4yWrDr/MdoeLABYGFIeJwKEMu0VNjtiNdQ1mbX31uWDuMfJyDpdTZ8aIhxSo7S4Oil7bvpbpmqEPHwd5j3iPK3DdAKhcBAkOfPur2FP3R3iO8bVVWn5noiqU/vsrQq2PCFHvnllFYpYKRTKpla0bxa9WdmRJhAvpgBdUfcQFoIrrDfvO9djA2yTTJxzbDcT3GAdLtvnR9zcaRrrNlSp0NHNrDVjxcSv5bGixB8KKKmt7IKOo/RB6YweBpN+UbKhKo6O5pRaiDohxYS05ncA8UJp+81fMqT6iNNr2vn0CZScqINi1rCy5xoroXMvwnrU/nY+ePB6j8YnZFnspY1LW831Bdz0JLTLeeZrtEOg/6GrfOcQuEQZ+FiqE3xo+cpETksVUvcj/hzGMCnjwtHKe6GM18Li2GfkdTT/6BebbvAFmPvKBdSMkrVS6oVGm3UbEzGo6dqKhHyKqplYvr7/3pThARRvMylERoICs+pf/UWjsfhN52jEBm/FImD6c=",
  "Group": "NOW"
}
```


Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Temp\name.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
C:\Users\user\AppData\Local\Temp\name.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$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\name.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
C:\Users\user\AppData\Local\Temp\name.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

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.492099585.0000000000DA0000.00000004.00000001.sdmp	JoeSecurity_AsyncRAT	Yara detected AsyncRAT	Joe Security	

Source	Rule	Description	Author	Strings
00000004.00000002.488368637.000000000087 2000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8 JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000004.00000002.488368637.000000000087 2000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000004.00000002.488368637.000000000087 2000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000004.00000002.498075697.000000000535 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
Click to see the 77 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.name.exe.31a89d8.4.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x2dbb:$x1: NanoCore.ClientPluginHost • 0x2de5:$x2: IClientNetworkHost
4.2.name.exe.31a89d8.4.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0x2dbb:$x2: NanoCore.ClientPluginHost • 0x4c6b:$s4: PipeCreated
4.2.name.exe.455fab8.19.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost
4.2.name.exe.455fab8.19.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost
4.2.name.exe.455fab8.19.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 168 entries				

Sigma Overview

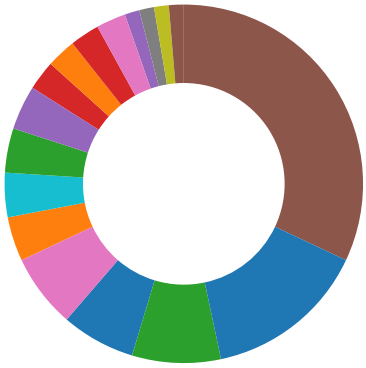
System Summary:

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
Yara detected Nanocore RAT
Machine Learning detection for dropped file

Compliance:

Detected unpacking (overwrites its own PE header)

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
Potential malicious VBS script found (has network functionality)

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected AsyncRAT

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)
.NET source code contains very large strings

Data Obfuscation:

Detected unpacking (overwrites its own PE header)
VBScript performs obfuscated calls to suspicious functions
.NET source code contains potential unpacker

Boot Survival:

Yara detected AsyncRAT

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

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

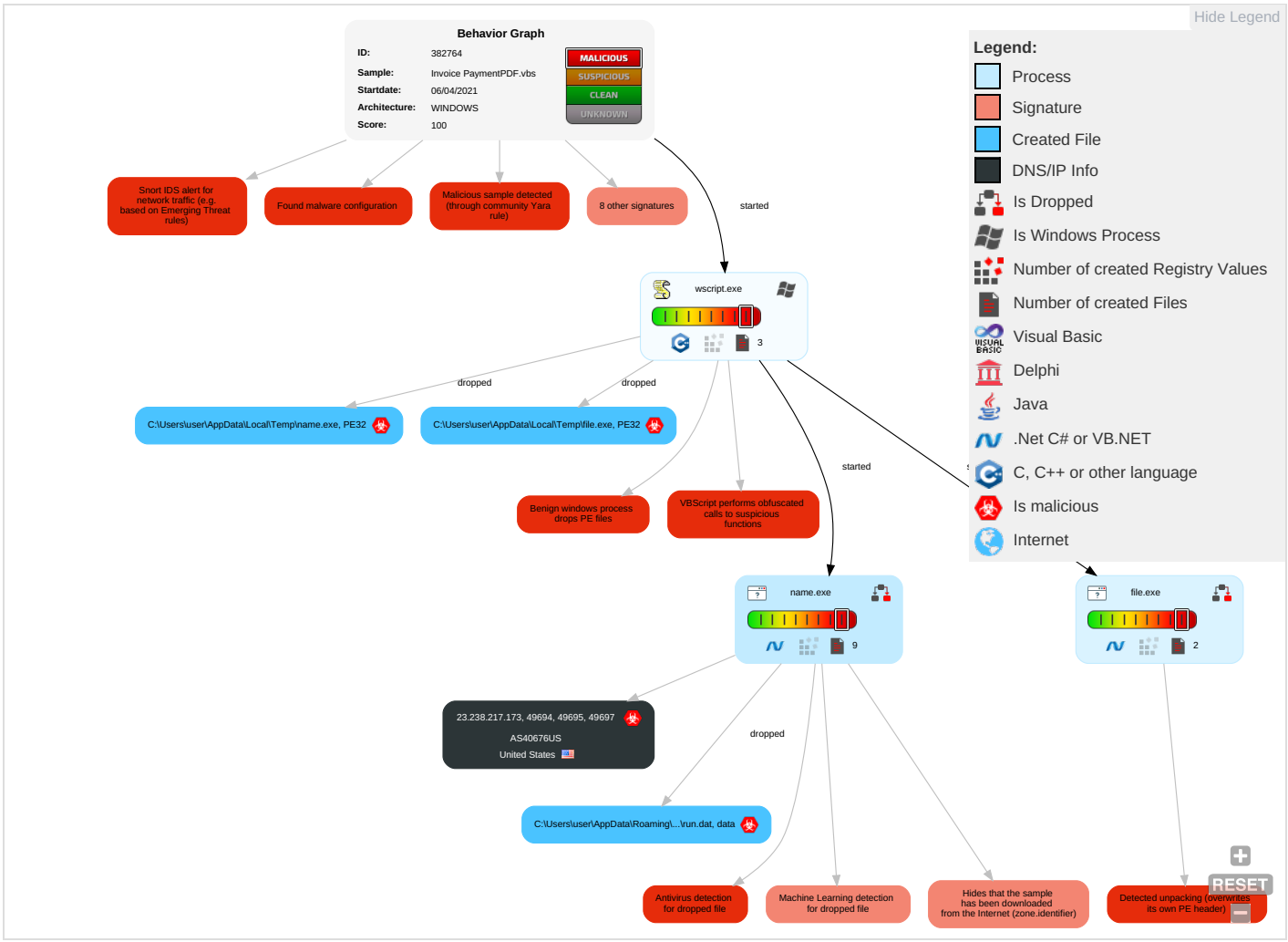
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 1	Input Capture 1 1	Query Registry 1	Remote Services	Input Capture 1 1	Exfiltration Over Other Network Medium	Non-S Port 1
Default Accounts	Scheduled Task/Job 1	DLL Side-Loading 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 3 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Remot Softwa
Domain Accounts	Scripting 2 2 1	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 3 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Stegar
Local Accounts	Exploitation for Client Execution 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Virtualization/Sandbox Evasion 3 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protoc Impers
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallba Chann
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2 1	Cached Domain Credentials	Remote System Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multib Comm
External Remote Services	Scheduled Task	Startup Items	Startup Items	Hidden Files and Directories 1	DCSync	File and Directory Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Comm Used F
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Obfuscated Files or Information 1 2	Proc Filesystem	System Information Discovery 1 3	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applic Layer
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Software Packing 2 2	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web P

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Comm and C
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	DLL Side-Loading 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Tr Protoc

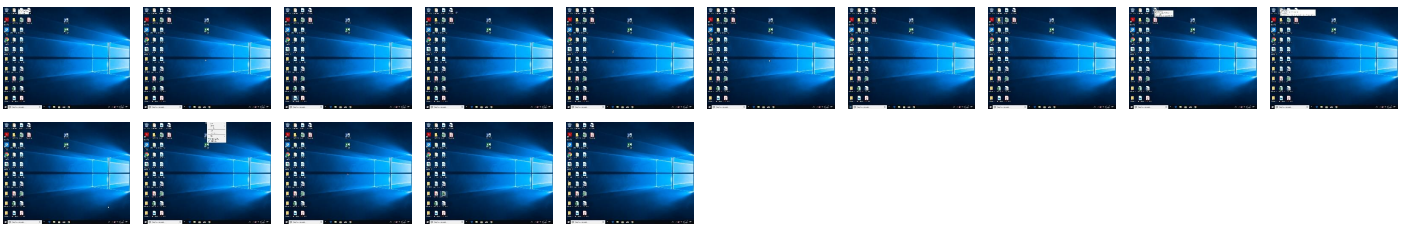
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\name.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
C:\Users\user\AppData\Local\Temp\name.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\file.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.name.exe.53f0000.23.unpack	100%	Avira	TR/NanoCore.fadte		Download File
4.0.name.exe.870000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
4.2.name.exe.870000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	file.exe, 00000003.00000002.492732344.0000000002911000.00000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
23.238.217.173	unknown	United States		40676	AS40676US	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	382764
Start date:	06.04.2021
Start time:	16:31:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 3s
Hypervisor based Inspection enabled:	false

Report type:	light
Sample file name:	Invoice PaymentPDF.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:	31
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winVBS@5/6@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.64.90.137, 184.30.21.144, 2.20.142.209, 2.20.142.210, 168.61.161.212, 184.30.24.56, 13.88.21.125, 20.50.102.62, 52.147.198.201, 40.88.32.150, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129, 104.42.151.234, 20.82.210.154 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, a767.dscg3.akamai.net, skypedataprdcoleus16.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:31:57	API Interceptor	994x Sleep call for process: name.exe modified
16:32:03	API Interceptor	1x Sleep call for process: file.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS40676US	g0g865fQ2S.exe	Get hash	malicious	Browse	• 172.107.55.6
	4xMdbgzeJQ.exe	Get hash	malicious	Browse	• 172.106.71.28
	DtE7OndZYB.exe	Get hash	malicious	Browse	• 104.217.62.116
	Gt8AN6GiOD.exe	Get hash	malicious	Browse	• 172.107.55.6
	1LHKlbcoW3.exe	Get hash	malicious	Browse	• 172.107.55.6
	ZwNJI24QAf.exe	Get hash	malicious	Browse	• 172.107.55.6
	MV Sky Marine_pdf.exe	Get hash	malicious	Browse	• 172.106.71.28
	quLdcfImUL.exe	Get hash	malicious	Browse	• 107.160.235.31
	Swift.exe	Get hash	malicious	Browse	• 107.160.235.31
	w.exe	Get hash	malicious	Browse	• 172.106.0.71
	7.exe	Get hash	malicious	Browse	• 172.106.0.71
	BSG_ptf.exe	Get hash	malicious	Browse	• 107.160.12 7.252
	Tax Invoice_309221.exe	Get hash	malicious	Browse	• 172.93.163.101
	bXSINeHUUZ.dll	Get hash	malicious	Browse	• 23.228.215.119
	PAYMENTSWIFT COPY.PDF.exe	Get hash	malicious	Browse	• 107.160.235.10
	Archivo.CarrefourOnliner.efasvtr.qKUjVasadm.vbs	Get hash	malicious	Browse	• 172.107.45.224
	smokeweed.vbs	Get hash	malicious	Browse	• 154.16.67.107
	jvHSccqW.exe	Get hash	malicious	Browse	• 154.16.67.107
	N5eld3tiba.exe	Get hash	malicious	Browse	• 172.107.43.174
	shed.exe	Get hash	malicious	Browse	• 172.106.24 2.148

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\AppData\Local\Temp\file.exe
File Type:	Microsoft Cabinet archive data, 58596 bytes, 1 file
Category:	dropped
Size (bytes):	58596
Entropy (8bit):	**7.995478615012125**
Encrypted:	**true**
SSDEEP:	1536:J7r25qSSheImS2zyCvg3nB/QPsBbgwYkGrLMQ:F2qSSwIm1m/QEBbgb1oQ
MD5:	61A03D15CF62612F50B74867090DBE79
SHA1:	15228F34067B4B107E917BEBAF17CC7C3C1280A8
SHA-256:	F9E23DC21553DAA34C6EB778CD262831E466CE794F4BEA48150E8D70D3E6AF6D
SHA-512:	5FECE89CCBBF994E4F1E3EF89A502F25A72F359D445C034682758D26F01D9F3AA20A43010B9A87F2687DA7BA201476922AA46D4906D442D56EB59B2B881259D3
Malicious:	false
Reputation:	high, very likely benign file
Preview:	MSCF.....,.....I.....T.....bR. .authroot.stl...s~.4..CK..8T....c_.d....A.K.....&.-.J...."Y...$E.KB..D...D.....3.n..u.....\|..=H4..c&.....f.,..=..-....p2.:..`HX.....b..... Di.a.....M.....4.....i..}..:~N.<..>.*.V..CX.....B.....,.q.M.....HB..E~Q...)..Gax../..}7..f.....O0...x..k..ha...y.K.0.h..(....{2Y.].g...yw..\|0.+?.`-../.xvy..e.....w.+^...w\|.Q.k.9&.Q.EzS.f.....>? w.G.....v.F.....A.....-P.$.Y...u....Z..g..>.0&.y.(..<.].`>... ..R.q...g.Y..s.y.B..B....Z.4.<?.R....1.8.<.=.8..[a.s.....add..).NtX....r....R.&W4.5]....k.._iK..xzW.w.M.>,5.}..}.tLX5Ls3_.. ).!..X.~...%.B.....YS9m.,.....BV`.Cee.....?.....:.x-.q9j...Yps..W...1.A<.X.O....7.ei..a\.~=X....HN.#....h,....y...\.br.8.y"k).....~B..v....GR.g|.z..+.D8.m..F .h...*.....ItNs.\....s...,f `D...]..k...:9..lk.<D....u.....[...*.wY.O....P?.U.l....Fc.ObLq.....Fvk..G9.8..!..\T:K`.....'.3.....;.u..h...uD..^.bS...r.....j..j .=...s .FxV....g.c.s..9.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\AppData\Local\Temp\file.exe
File Type:	data
Category:	modified
Size (bytes):	326

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Entropy (8bit):	3.1120436261832696
Encrypted:	false
SSDEEP:	6:kK+fkwTJ6YN+SkQlPlEGYRMY9z+4KIDA3RUe0ht:GkwTJ6HkPlE99SNxAhUe0ht
MD5:	BA0575EB4D46A9D8A3A8E2398BF53D2F
SHA1:	324F765E21FDA9DC079940097B03F1D022C95E87
SHA-256:	33C4B79161DB3CE59A51170AD656296A29CD535695C83703060A29995D3B0156
SHA-512:	75F23A24AEA6A305ECB4FC113565E396AA282ED5860ACAAFC298F7C4CEDC80F509EFEF6302D73CED0AB0E8C93E622D1C79BD6111BC7534BEDA2FEE4A7F901295
Malicious:	false
Reputation:	low
Preview:	p..... .....c..=+..(..... .....$.....h.t.t.p.:.//./.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.d.8.f.4.f.3.f.6.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Temp\file.exe	
Process:	C:\Windows\System32\wscript.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	253952
Entropy (8bit):	5.107675207273867
Encrypted:	false
SSDEEP:	3072:vrdQJkVIb71u5aEYLUfh5+u/0a2HBrvyIBfn8+ux221Hl:OJk071cacfh5+CJK+
MD5:	76D2BB0F57BBF02E190055FCDB3663DB
SHA1:	D2AC68C0F7284EA67072BD396D1CC20A83BE4D95
SHA-256:	B1BD43F34BFCC14D04E27D65D0CEFC7064BCC536758B6CA48F0F786040EFAA71
SHA-512:	F848C3CEFE0BA112F4BA80427785E9654EC22F0625FCD30892C00949EE98E83517C334FE5A5F8E96A03C1149D7B05DCFE50CE460E52EE0C519AAFB689168D8BF
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....<I`..... ... ....@.. .....@..... ..@.....W.... ..... ..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.reloc..... .....@..B.....H..... .....~....(....o.....o....(....*.r...pr...pr...po....r...pr...po....(.....*..(....*...BSJB.....v4.0.30319 .....l...0...#~.....#Strings.....#US.....#GUID.....0...#Blob.....W.....%3.....G.@...r.`.....`...6.`...S.`...r.`.....`.....`... ..`.....`...R.8.....`.....`.....@.....`.....@...

C:\Users\user\AppData\Local\Temp\name.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):	7.4478668113025845
Encrypted:	false
SSDEEP:	6144:wLV6Bta6dtJmakIM5fFmHi8ieZv00yRQ+E2c6:wLV6BtpmksFmC83KWH2c6
MD5:	50B53CECA7021AD9ABEA4074A634680A
SHA1:	90A934B90A726E47625451C58417BB4314730C41
SHA-256:	72FFB8177D08CF4E454B1E38FD83BC8681FD5FFE91336BC3D3611EE9823FD498
SHA-512:	B7E6D8F4AA99CF2FAB81A1EB7CAE6191C95B2D52FD1D5B4B7093483A283F59AC2A1AACFFA332E83890815541AEAC6B4B06A02B93DADE9A64820124F870F7138D
Malicious:	**true**
Yara Hits:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\name.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\name.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\name.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\name.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100%
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\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\AppData\Local\Temp\name.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Size (bytes):	2088
Entropy (8bit):	7.089541637477408
Encrypted:	false
SSDEEP:	48:IknjhUknjhUknjhUknjhUknjhUknjhUknjhUknjhL:HjhDjhDjhDjhDjhDjhDjhDjhL
MD5:	84864902DEC5038CEF326FF21E8D5F98
SHA1:	2F10FEC81D95813C3B2530EC4CECED70164A08C5
SHA-256:	5B4853A46F99AC6445B68DC1A841D511D0E86C6EDEC2A0A84F3778039A578B6B
SHA-512:	A77BCDB522CE208C8D785F44D9FE90C6D1314CB199A4BE72E220F4B8C5446265EEEF1C51EFFD2D7BDCCDC8F4A76F803A41A4973364757950D0777E8BAEF0B1 4C
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?...A.K...J.=8x!....+ .2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH}..../H......L...?. ..A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f...p............:7rH }..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.... S....}FF.2...h.M+....L.#.X..+......*....~f.G0^..;....W2.=...K.~.L..&f. ..p............:7rH}..../H......L...?...A.K...J.=8x!....+.2e'..E?.G......[.&Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b........4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\AppData\Local\Temp\name.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:8htn:y
MD5:	FB6B1642D0452C3108CB83017340C8F1
SHA1:	2F9FC413A65B9F3B720266284A7360657E30E17D
SHA-256:	29346F09E16F22AE462C50E61036CC88A2CF0CB789D7895EEF9B1CBEB379EB84
SHA-512:	9828FBF3A07A76A41839634FCC5DE7A6E4696729A9401012228FF01C0D4B8F66AADA3875086F9D8C570ECD947037077A7CD331AA486F59EED0523BBB47D7ADF
Malicious:	**true**
Reputation:	low
Preview:	...+T..H

Static File Info

General

File type:	ASCII text, with very long lines, with CRLF line t erminators
Entropy (8bit):	5.345616839723832
TrID:	• Visual Basic Script (13500/0) 87.10% • Disk Image (Macintosh), GPT (2000/0) 12.90%
File name:	Invoice PaymentPDF.vbs
File size:	678447
MD5:	3911ee0964b7aa57b411fe3d88d304d6
SHA1:	b6f21d1f4a6f3329e8403038906fc93a7872fcee
SHA256:	ea5784a4389f86bb28ec9ca5fc099b5d4e8791983ce7b66 df5c1cf8cb01e5952
SHA512:	bf206257cd473d35a751f1802aba1f7f10f87ef94ffd92bd7 c8d001bf07e5335c66a92d743c941445dc37eb23bc7fec6 343b3e4cf446d7cadf989c1d0ca005fc
SSDEEP:	12288:irzreo/goc/lNlQiBsrvGnCH6wonm724W1VVh8FE fZkKw:UregH4NW8srvGCa5trV0FwkB
File Content Preview:	on error resume next..Dim JpeJpoKJowKEZgOlpSmLm JSzleJKfhfZVmevyiVZPhyddgTpiapRcRLAXeXLezdHRlj nCTnGwMvELoWFKTcFrNxDaeYTKKuPErMsxgnPmjV PVHoiISAKXYPEnfNYuUwlRgAUcdHegNSIriiTpqLsJksf bIFSTPUSnjxpGUFeKWeJGHMExtjEIEbhnUsUYpKRsz VIlsMU..'kghnGiZTvAUZfQKiHQBlblFULM

File Icon

Icon Hash:	e8d69ece869a9ec4

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/06/21-16:31:59.464981	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49694	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:03.421526	TCP	2030673	ET TROJAN Observed Malicious SSL Cert (AsyncRAT Server)	6606	49695	23.238.217.173	192.168.2.7
04/06/21-16:32:05.489425	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49697	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:12.060625	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49698	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:18.068574	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49705	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:24.411153	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49709	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:28.964583	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:36.130837	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49720	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:40.669412	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49724	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:46.808761	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:52.822544	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49729	54999	192.168.2.7	23.238.217.173
04/06/21-16:32:58.962642	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49738	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:05.180390	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:09.773608	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:14.353287	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:21.303198	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49753	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:27.525754	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49754	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:32.134776	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49755	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:38.233306	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49756	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:44.457596	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49759	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:50.533266	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49760	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:55.244682	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49761	54999	192.168.2.7	23.238.217.173
04/06/21-16:33:59.826832	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49762	54999	192.168.2.7	23.238.217.173

Network Port Distribution

Total Packets: 79

- 53 (DNS)
- 54999 undefined

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 16:31:59.144707918 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:31:59.308810949 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:31:59.309655905 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:31:59.464981079 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:31:59.649559021 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:31:59.650315046 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:31:59.875344038 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:31:59.875505924 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.040448904 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.040903091 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.267366886 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.267471075 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.487400055 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.487564087 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.494333982 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.494363070 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.494375944 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.494393110 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.494482040 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.494499922 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.660765886 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.660799026 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.660820007 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.660840034 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.660861015 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.660861015 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.660897017 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.660916090 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.660922050 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.660942078 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.660944939 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.660970926 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.660998106 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825064898 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825093031 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825115919 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825136900 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825145960 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825158119 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825179100 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825182915 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825206041 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825222015 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825227022 CEST	54999	49694	23.238.217.173	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 16:32:00.825248957 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825249910 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825269938 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825287104 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825290918 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825314045 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825320959 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825335979 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825361013 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825361013 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825397968 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825406075 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825421095 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.825437069 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.825469971 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.990700006 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990727901 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990741968 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990756035 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990772009 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990787983 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990793943 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.990806103 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990824938 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990843058 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990849018 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.990859985 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990878105 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.990880013 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990899086 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990906000 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.990916014 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990931988 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.990932941 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990951061 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990962982 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.990967035 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990983963 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.990999937 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.991002083 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991023064 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991034985 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.991040945 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991059065 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991065979 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.991075039 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991091967 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991099119 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.991108894 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991126060 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991128922 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.991142988 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991152048 CEST	49694	54999	192.168.2.7	23.238.217.173
Apr 6, 2021 16:32:00.991163015 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991180897 CEST	54999	49694	23.238.217.173	192.168.2.7
Apr 6, 2021 16:32:00.991190910 CEST	49694	54999	192.168.2.7	23.238.217.173

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 16:31:46.956240892 CEST	62452	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:31:47.002151966 CEST	53	62452	8.8.8.8	192.168.2.7
Apr 6, 2021 16:31:49.708651066 CEST	57820	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:31:49.767714977 CEST	53	57820	8.8.8.8	192.168.2.7

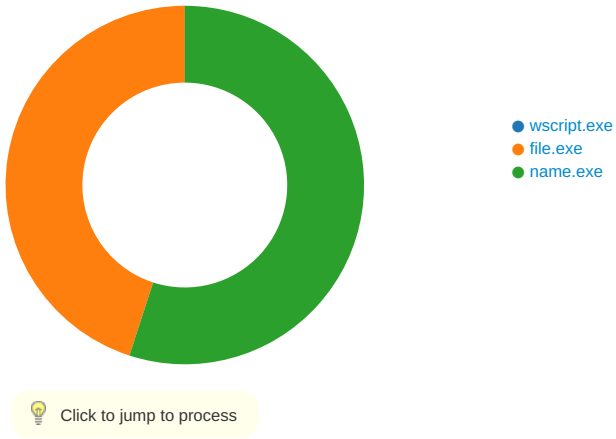
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 16:32:04.124748945 CEST	50848	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:04.182363033 CEST	53	50848	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:15.063349009 CEST	61242	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:15.112181902 CEST	53	61242	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:16.151714087 CEST	58562	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:16.208039999 CEST	53	58562	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:16.225825071 CEST	56590	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:16.271897078 CEST	53	56590	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:17.452346087 CEST	60501	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:17.504942894 CEST	53	60501	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:18.735611916 CEST	53775	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:18.785016060 CEST	53	53775	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:19.834711075 CEST	51837	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:19.889540911 CEST	53	51837	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:20.993029118 CEST	55411	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:21.042897940 CEST	53	55411	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:26.621511936 CEST	63668	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:26.672574043 CEST	53	63668	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:28.742068052 CEST	54640	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:28.789588928 CEST	53	54640	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:30.523845911 CEST	58739	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:30.570034027 CEST	53	58739	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:31.304320097 CEST	60338	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:31.353317022 CEST	53	60338	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:32.524560928 CEST	58717	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:32.570400953 CEST	53	58717	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:33.645565987 CEST	59762	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:33.691447020 CEST	53	59762	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:34.718178988 CEST	54329	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:34.764749050 CEST	53	54329	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:35.502871037 CEST	58052	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:35.551671982 CEST	53	58052	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:36.580980062 CEST	54008	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:36.626964092 CEST	53	54008	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:37.516587019 CEST	59451	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:37.564519882 CEST	53	59451	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:39.747912884 CEST	52914	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:39.794955969 CEST	53	52914	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:40.890270948 CEST	64569	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:40.940371990 CEST	53	64569	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:42.571144104 CEST	52816	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:42.627120018 CEST	53	52816	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:42.650916100 CEST	50781	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:42.709528923 CEST	53	50781	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:54.902240992 CEST	54230	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:54.959589958 CEST	53	54230	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:55.588939905 CEST	54911	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:55.644551039 CEST	53	54911	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:56.063314915 CEST	49958	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:56.125809908 CEST	50860	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:56.126456022 CEST	53	49958	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:56.184194088 CEST	53	50860	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:56.654314995 CEST	50452	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:56.708714962 CEST	53	50452	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:57.310209990 CEST	59730	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:57.358108997 CEST	53	59730	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:57.946122885 CEST	59310	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:58.003563881 CEST	53	59310	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:58.504122019 CEST	51919	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:58.558964014 CEST	53	51919	8.8.8.8	192.168.2.7
Apr 6, 2021 16:32:59.549380064 CEST	64296	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:32:59.609319925 CEST	53	64296	8.8.8.8	192.168.2.7
Apr 6, 2021 16:33:00.874543905 CEST	56680	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:33:00.928958893 CEST	53	56680	8.8.8.8	192.168.2.7

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 6, 2021 16:33:01.924225092 CEST	58820	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:33:01.978292942 CEST	53	58820	8.8.8.8	192.168.2.7
Apr 6, 2021 16:33:07.199218988 CEST	60983	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:33:07.257049084 CEST	53	60983	8.8.8.8	192.168.2.7
Apr 6, 2021 16:33:13.683300018 CEST	49247	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:33:13.729132891 CEST	53	49247	8.8.8.8	192.168.2.7
Apr 6, 2021 16:33:14.862555981 CEST	52286	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:33:14.908555984 CEST	53	52286	8.8.8.8	192.168.2.7
Apr 6, 2021 16:33:17.566824913 CEST	56064	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:33:17.612814903 CEST	53	56064	8.8.8.8	192.168.2.7
Apr 6, 2021 16:33:39.852117062 CEST	63744	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:33:39.898274899 CEST	53	63744	8.8.8.8	192.168.2.7
Apr 6, 2021 16:33:43.389631987 CEST	61457	53	192.168.2.7	8.8.8.8
Apr 6, 2021 16:33:43.454875946 CEST	53	61457	8.8.8.8	192.168.2.7

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: wscript.exe PID: 5648 Parent PID: 3292

General

Start time:	16:31:53
Start date:	06/04/2021
Path:	C:\Windows\System32\wscript.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\wscript.exe 'C:\Users\user\Desktop\Invoice PaymentPDF.vbs'
Imagebase:	0x7ff6e8cd0000
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: 00000000.00000003.221036890.0000028C2F7DD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.221036890.0000028C2F7DD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.221036890.0000028C2F7DD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.221395842.0000028C2F7BC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.221395842.0000028C2F7BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.221395842.0000028C2F7BC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.225834139.0000028C2F7B2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.225834139.0000028C2F7B2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.225834139.0000028C2F7B2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.221500985.0000028C2F7BC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.221500985.0000028C2F7BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.221500985.0000028C2F7BC000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.221285702.0000028C2F8E7000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.221285702.0000028C2F8E7000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.221285702.0000028C2F8E7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.225899093.0000028C2F7B4000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.225899093.0000028C2F7B4000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.225899093.0000028C2F7B4000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.225743694.0000028C2F7B2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.225743694.0000028C2F7B2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.225743694.0000028C2F7B2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.229634460.0000028C2F7B6000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.229634460.0000028C2F7B6000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.229634460.0000028C2F7B6000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000002.230491203.0000028C2FC10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.230491203.0000028C2FC10000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.230491203.0000028C2FC10000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.221435986.0000028C2F7BC000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.221435986.0000028C2F7BC000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.221435986.0000028C2F7BC000.00000004.00000001.sdmp,

	Author: Kevin Breen <kevin@techanarchy.net>
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: file.exe PID: 360 Parent PID: 5648

General

Start time:	16:31:56
Start date:	06/04/2021
Path:	C:\Users\user\AppData\Local\Temp\file.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user~1\AppData\Local\Temp\file.exe'
Imagebase:	0x650000
File size:	253952 bytes
MD5 hash:	76D2BB0F57BBF02E190055FCDB3663DB
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: 00000003.00000002.492099585.0000000000DA0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AsyncRAT, Description: Yara detected AsyncRAT, Source: 00000003.00000002.492732344.0000000002911000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
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	7FFF8A72F1E9	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	7FFF8A72F1E9	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

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	7FFF8A5FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	7FFF8A5FB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\mscorlib\ac26e2af62f23e37e645b5e44068a025\mscorlib.ni.dll.aux	unknown	176	success or wait	1	7FFF8A6D12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF8A602625	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a171 39182a9efd561f01fada9688a5\System.ni.dll.aux	unknown	620	success or wait	1	7FFF8A6D12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	7FFF8A5FB9DD	unknown
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	7FFF8A5FB9DD	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Core\4 e05e2e48b8a6dd267a8c9e25ef129a7\System.Core.ni.dll.aux	unknown	900	success or wait	1	7FFF8A6D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Config uration\e82398e9ff6885d617e4b97e31fb4f02\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	7FFF8A6D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Xml\f2 e3165e3c718b7ac302fea40614c984\System.Xml.ni.dll.aux	unknown	748	success or wait	1	7FFF8A6D12E7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	7FFF8955B526	ReadFile
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	7FFF8955B526	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\Microsoft.V99 21e851#\f2e0589ed6d670f264a5f65dd0ad000f\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	7FFF8A6D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Window s.Forms\6d7d43e19d7fc0006285b85b7e2c8702\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	7FFF8A6D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Drawin g\49e5c0579db170be9741dccc34c1998e\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	7FFF8A6D12E7	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_64\System.Manage ment\d0f4eb5b1d0857aabc3e7dd079735875\System.Management.ni.dll.aux	unknown	764	success or wait	1	7FFF8A6D12E7	ReadFile

Analysis Process: name.exe PID: 4704 Parent PID: 5648

General

Start time:	16:31:56
Start date:	06/04/2021
Path:	C:\Users\user\AppData\Local\Temp\name.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user~1\AppData\Local\Temp\name.exe'
Imagebase:	0x870000
File size:	207360 bytes
MD5 hash:	50B53CECA7021AD9ABEA4074A634680A
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: 00000004.00000002.488368637.0000000000872000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.488368637.0000000000872000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.488368637.0000000000872000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.498075697.0000000005350000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.498075697.0000000005350000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000000.224566255.0000000000872000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000000.224566255.0000000000872000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000000.224566255.0000000000872000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.496683014.0000000004121000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.496683014.0000000004121000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499346217.0000000006090000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499346217.0000000006090000.00000004.00000001.sdmp, Author: Florian Roth • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499421831.00000000060B0000.00000004.00000001.sdmp, Author:

Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499421831.00000000060B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499738147.0000000006130000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499738147.0000000006130000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.496940045.0000000004180000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499506024.00000000060E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499506024.00000000060E0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499468188.00000000060D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499468188.00000000060D0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499649903.0000000006110000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499649903.0000000006110000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.495651138.00000000032CF000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.498280487.00000000053F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.498280487.00000000053F0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.498280487.00000000053F0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499439441.00000000060C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499439441.00000000060C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.494696991.0000000003173000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.498013207.0000000005320000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.498013207.0000000005320000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.497731455.000000000455A000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.497731455.000000000455A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499285834.0000000006070000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499285834.0000000006070000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499244411.0000000006050000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499244411.0000000006050000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499588089.0000000006100000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499588089.0000000006100000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.499782274.0000000006160000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000004.00000002.499782274.0000000006160000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000004.00000002.497341701.00000000042F7000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\name.exe, Author: Florian Roth • Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\name.exe, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: C:\Users\user\AppData\Local\Temp\name.exe, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: C:\Users\user\AppData\Local\Temp\name.exe, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML
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	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2DB08ED	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	2DB09E7	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\Logs	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	2DB08ED	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	2DB08ED	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	724660AC	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	724660AC	unknown
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	2DB09E7	CreateFileW

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	ef 1a 90 2b 54 f9 d8 48	...+T..H	success or wait	1	2DB0B9F	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	1	2DB0B9F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc bb 8e f9 04 20 53 f0 bc 12 1c d2 7d 46 46 d4 32 d7 fe a4 68 e2 b4 4d 2b cf cc b9 c1 ec 4c bb 23 8c 58 cb ee 2b 8b b7 cd 01 a9 c0 2a c7 f9 1e d1 7e 66 1e 47 30 5e c3 a9 dd 96 3b b4 2e 95 a2 57 32 c2 3d 10 b3 ce 4b ca 7e c7 4c cc 9f 15 26 66 8d bb 2e 70 c8 04 1b f8 b7 c2 0f e9 ff e7 0b 10 3a 37 72 48 7d bd be f1 88 0d 2f 48 16 b2 87 06 17 96 4c 8c b6 04 3f b5 f3 04 41 08 4b 07 d1 e5 84 4a 17 3d 38 78 21 19 a1 e1 e4 2b fa 32 65 27 d7 1f 45 3f d9 47 11 9e a7 e7 a8 01 f0 5b 00 26	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i..... S.....}FF.2.. .h..M+.....L.#.X..+.....*.... ~f.G0^....;....W2.=...K.~.L... &f...p.....:7rH}...../H .....L...?...A.K....J.=8x!... .+.2e'..E?.G.....[.&	success or wait	8	2DB0B9F	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	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72498738	ReadFile
C:\Users\user\AppData\Local\Temp\name.exe	unknown	4096	success or wait	1	7253BF06	unknown
C:\Users\user\AppData\Local\Temp\name.exe	unknown	512	success or wait	1	7253BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72495544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2DB0B9F	ReadFile
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7253BF06	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7253BF06	unknown

Disassembly

Code Analysis