ID: 321681
Sample Name: 4yGRcXEf.exe
Cookbook: default.jbs
Time: 14:48:24
Date: 23/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

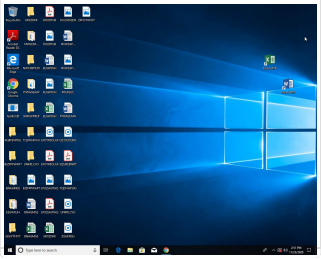
Analysis Report 4yGRcXEf.exe

Overview

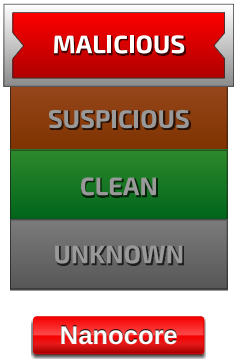
General Information

Sample Name:	4yGRcXEf.exe
Analysis ID:	321681
MD5:	87e77797615466..
SHA1:	9cd228af2ea1f50..
SHA256:	d50a35f05df59b5..
Tags:	exe NanoCore

Most interesting Screenshot:



Detection

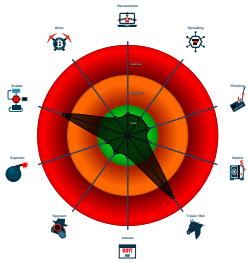


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Detected Nanocore Rat
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e….
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Machine Learning detection for samp…
- Uses dynamic DNS services
- Antivirus or Machine Learning detec…

Classification



Startup

- **System is w10x64**
- 4yGRcXEf.exe (PID: 6748 cmdline: 'C:\Users\user\Desktop\4yGRcXEf.exe' MD5: 87E77797615466BAA21CDE3F7BB347F2)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
4yGRcXEf.exe	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
4yGRcXEf.exe	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
4yGRcXEf.exe	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
4yGRcXEf.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
00000000.00000000.224571570.00000000002B2000.00000002.00020000.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0xff8d:$x1: NanoCore.ClientPluginHost 0xffca:$x2: IClientNetworkHost 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000000.224571570.00000000002B2000.00000002.00020000.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000000.224571570.00000000002B2000.00000002.00020000.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0xfcf5:$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
00000000.00000003.233132403.0000000004534000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	0x5cc77:$a: NanoCore 0x5cc9c:$a: NanoCore 0x5ccf5:$a: NanoCore 0x6ce94:$a: NanoCore 0x6ceba:$a: NanoCore 0x6cf16:$a: NanoCore 0x79d6d:$a: NanoCore 0x79dc6:$a: NanoCore 0x79df9:$a: NanoCore 0x7a025:$a: NanoCore 0x7a0a1:$a: NanoCore 0x7a6ba:$a: NanoCore 0x7a803:$a: NanoCore 0x7acd7:$a: NanoCore 0x7afbe:$a: NanoCore 0x7afd5:$a: NanoCore 0x83e79:$a: NanoCore 0x83ef5:$a: NanoCore 0x867d8:$a: NanoCore 0x8bda1:$a: NanoCore 0x8be1b:$a: NanoCore

Source	Rule	Description	Author	Strings
Process Memory Space: 4yGRcXEf.exe PID: 6748	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x16ecd8:$x1: NanoCore.ClientPluginHost • 0x20fc2b:$x1: NanoCore.ClientPluginHost • 0x21a545:$x1: NanoCore.ClientPluginHost • 0x22d0c0:$x1: NanoCore.ClientPluginHost • 0x23010f:$x1: NanoCore.ClientPluginHost • 0x2354c3:$x1: NanoCore.ClientPluginHost • 0x238918:$x1: NanoCore.ClientPluginHost • 0x23b503:$x1: NanoCore.ClientPluginHost • 0x2426a7:$x1: NanoCore.ClientPluginHost • 0x247502:$x1: NanoCore.ClientPluginHost • 0x253cdc:$x1: NanoCore.ClientPluginHost • 0x26f67c:$x1: NanoCore.ClientPluginHost • 0x27e037:$x1: NanoCore.ClientPluginHost • 0x16ed39:$x2: IClientNetworkHost • 0x20fc6d:$x2: IClientNetworkHost • 0x21a58a:$x2: IClientNetworkHost • 0x22d11d:$x2: IClientNetworkHost • 0x23016c:$x2: IClientNetworkHost • 0x235520:$x2: IClientNetworkHost • 0x23b76f:$x2: IClientNetworkHost • 0x242704:$x2: IClientNetworkHost
Click to see the 2 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.4yGRcXEf.exe.2b0000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.0.4yGRcXEf.exe.2b0000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
0.0.4yGRcXEf.exe.2b0000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.0.4yGRcXEf.exe.2b0000.0.unpack	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

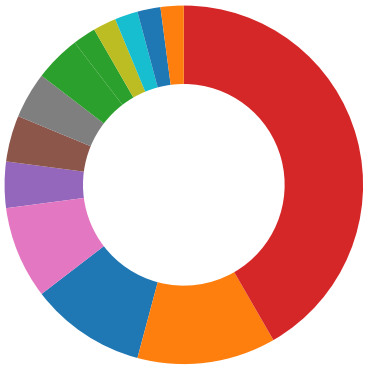
Sigma Overview

System Summary:

Sigma detected: NanoCore

Signature Overview

- AV Detection



- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- 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 / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Yara detected Nanocore RAT
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- Uses dynamic DNS services

E-Banking Fraud:

- Yara detected Nanocore RAT

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

- Hides that the sample has been downloaded from the Internet (zone.identifier)

Stealing of Sensitive Information:

- Yara detected Nanocore RAT

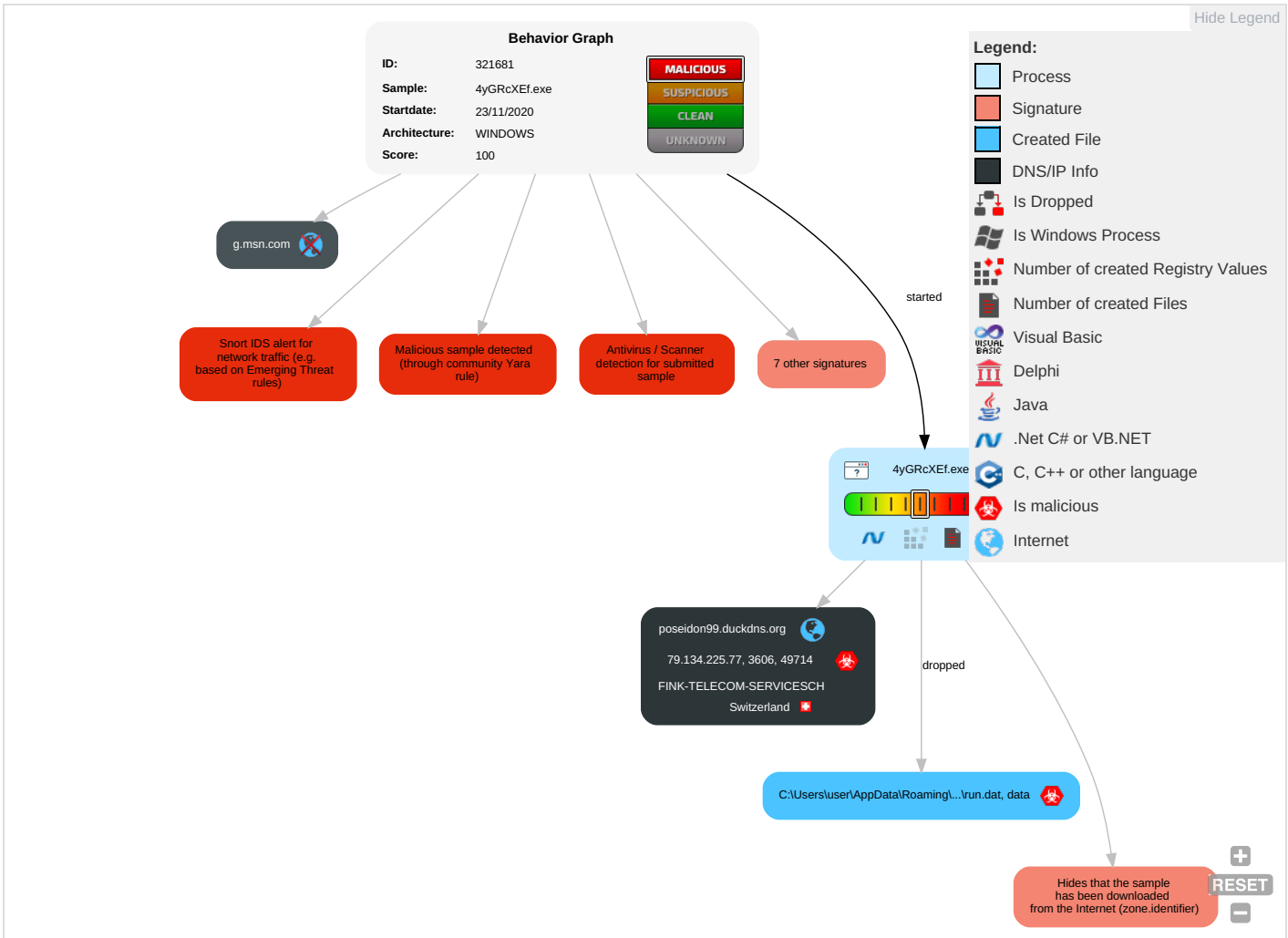
Remote Access Functionality:

- Detected Nanocore Rat
- Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation 1	Path Interception	Process Injection 1	Masquerading 1	OS Credential Dumping	Security Software Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Non-Standard Port 1	Eavesdrop o Insecure Network Communicat
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit SS7 Redirect Phc Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 1	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 1	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	System Information Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicat
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Poin

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
4yGRcXEf.exe	78%	Virustotal		Browse
4yGRcXEf.exe	100%	Avira	TR/Dropper.MSIL.Gen7	
4yGRcXEf.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.4yGRcXEf.exe.2b0000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

Source	Detection	Scanner	Label	Link
poseidon99.duckdns.org	1%	Virustotal		Browse

URLs

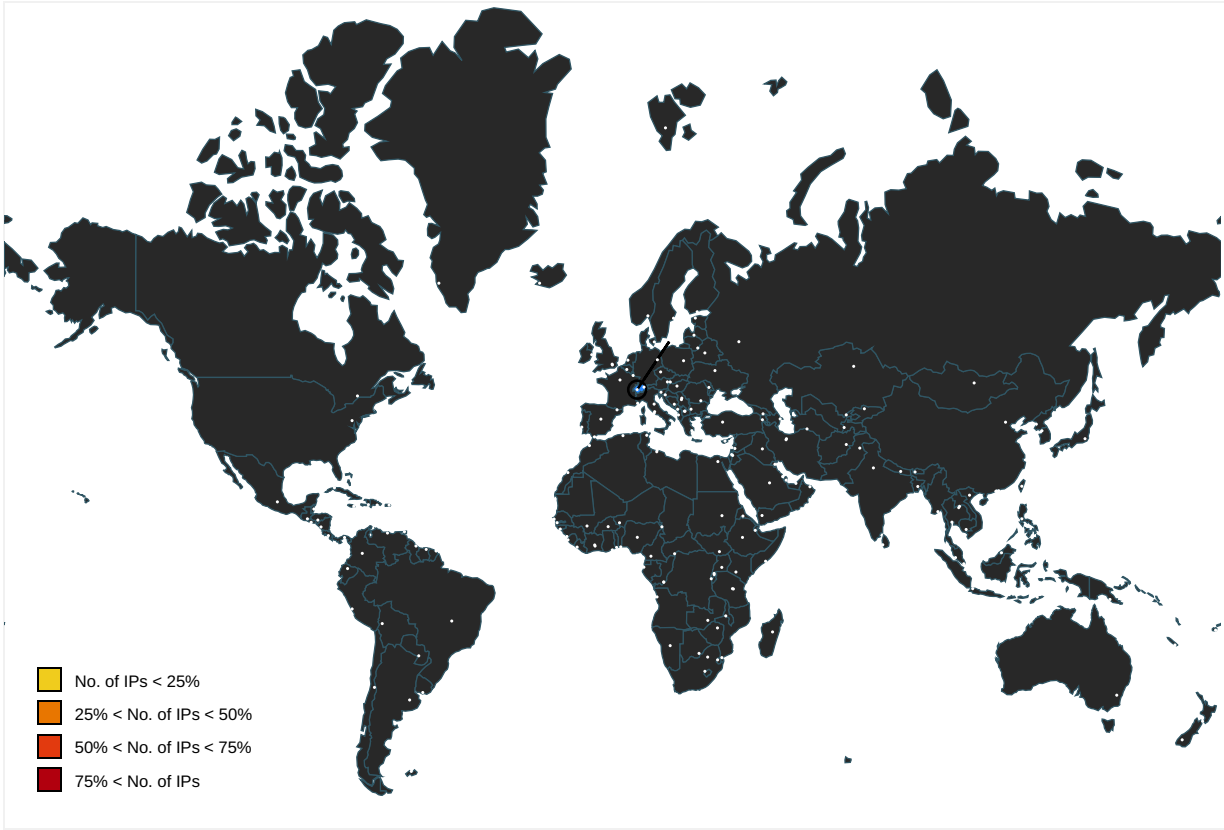
No Antivirus matches

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
poseidon99.duckdns.org	79.134.225.77	true	true	• 1%, Virustotal, Browse	unknown
g.msn.com	unknown	unknown	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.77	unknown	Switzerland		6775	FINK-TELECOM-SERVICESCH	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	321681
Start date:	23.11.2020
Start time:	14:48:24
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	4yGRcXEf.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	18
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@1/4@2/1
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: .exe

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • TCP Packets have been reduced to 100 • Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 104.43.139.144, 52.255.188.83, 23.210.248.85, 51.104.144.132, 20.54.26.129, 67.26.83.254, 8.248.131.254, 67.26.81.254, 8.253.95.121, 8.241.9.126, 40.67.254.36, 51.104.139.180, 52.142.114.176, 92.122.213.247, 92.122.213.194 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, wns.notify.windows.com.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, g-msn-com-nsatc.trafficmanager.net, par02p.wns.notify.windows.com.akadns.net, db5p.wns.notify.windows.com.akadns.net, emea1.notify.windows.com.akadns.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
14:49:13	API Interceptor	1051x Sleep call for process: 4yGRcXEf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
79.134.225.77	v#Uacac#Uc801#Uc694#Uccad_#Ud574#Uc131 _ PO_55956999.exe	Get hash	malicious	Browse	
	Transacion_CUS_REF_referencia es 000008223084566.vbe	Get hash	malicious	Browse	
	http://https://onedrive.live.com/download?cid=7FA2284F7D5167FA&resid=7FA2284F7D5167FA%21107&authkey=AIqIeyp5gnwLAeY	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
FINK-TELECOM-SERVICESCH	ORDER #201120A.exe	Get hash	malicious	Browse	• 79.134.225.92
	sSz5RnWs7F.exe	Get hash	malicious	Browse	• 79.134.225.40
	Scan_202011200113(1)xls.exe	Get hash	malicious	Browse	• 79.134.225.9
	3CAUxk3Je9.exe	Get hash	malicious	Browse	• 79.134.225.40
	Fl0aIIH39W.exe	Get hash	malicious	Browse	• 79.134.225.40
	NEW ORDER_8876630.exe	Get hash	malicious	Browse	• 79.134.225.9
	9Pimjl3jyq.exe	Get hash	malicious	Browse	• 79.134.225.40
	7tRM7RUC.exe	Get hash	malicious	Browse	• 79.134.225.99
	PURCHASE_ORDER.exe	Get hash	malicious	Browse	• 79.134.225.87
	YW2l1lBx5p2U84V.exe	Get hash	malicious	Browse	• 79.134.225.54
	ORDER #201006.exe	Get hash	malicious	Browse	• 79.134.225.92
	2HchQQHbc3.exe	Get hash	malicious	Browse	• 79.134.225.40
	http://https://uc13b1859d0dd1d287abe11849bc.dl.dropboxusercontent.com/cd/0/get/BDYpKT2DghcT8k6q6ivr3Z10tH2flzZ-quVnhNkvIaMzr65_x9Jb73dlKfp9-u2XxKjvY5mHqB-sTtfsf3X_DzOrS8DLCyWkeoM0ivsy2MmAb_UnT8m5tcbdlCmtPw__0Gg/file?dl=1	Get hash	malicious	Browse	• 79.134.225.8
	JfBrVoAbZJ.exe	Get hash	malicious	Browse	• 79.134.225.12
	hLP6IkkrSG.exe	Get hash	malicious	Browse	• 79.134.225.45
	Payment Confirmation NOV-85869983TGTTAS.exe	Get hash	malicious	Browse	• 79.134.225.14
	P9hBKKQw3T.exe	Get hash	malicious	Browse	• 79.134.225.110
	uqR1VNxNJn.exe	Get hash	malicious	Browse	• 79.134.225.52
	ORDER-#00654.doc.....exe	Get hash	malicious	Browse	• 79.134.225.92
	7GAi7ZFQz8.exe	Get hash	malicious	Browse	• 79.134.225.92

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\4yGRcXEf.exe
File Type:	data
Category:	dropped
Size (bytes):	248
Entropy (8bit):	7.094528505897445
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7r3l3TmKEt5mT1DhFtMhXvvHOxHB3GDq:X4LEnybgCFCtvd7bl3ThE4T19FtMhXvs
MD5:	061E700FE27D852034A5A44BF5985CCF
SHA1:	15B072DE6D6FDD92AE36F074345FA41985833E8D
SHA-256:	4BBB88AF530693EB4A710B0591D4BAF585837242C5690F5A821BF2FC9CC587CD
SHA-512:	CF6C5458AB50C859740490985D1E7E887D1116F3FA947FF2EC49AF9997A42F3402C63EF42B93498544195D9859FBB19CCC295966564B30F5ADB4A36D4E8886C6
Malicious:	false
Reputation:	low
Preview:	Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL....f.Z#.|...@HkG....G..O*V.....pz....".....r...w&&|..c..3}~.....~...os..f.....4..1.gJ.'.d".L....A.t...F.{....C.|&.w

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\4yGRcXEf.exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:rV:Z
MD5:	0F05952A6BB6C5B4C2017E0EBF8B67D9
SHA1:	0553EE2EBE7C542B6F063452E85248D8FF8DD8B0

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
SHA-256:	989124C5F8B84DCBD642AA1CA3811E5ACF5166D34093E64E51706D63F8EF50BA
SHA-512:	D9828A7219D5385F5B703230073EE9CAA08E9B14DDE7FC0A7D811ACEF745AFF1BAFE94D7F457223065559F30E1D25DA12A4A3662C8761DBA5C778957E95288A
Malicious:	**true**
Reputation:	low
Preview:	.(.....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\4yGRcXEf.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	5.153055907333276
Encrypted:	false
SSDEEP:	3:9bzY6oRDT6P2bfVn1:RzWDT621
MD5:	4E5E92E2369688041CC82EF9650EDED2
SHA1:	15E44F2F3194EE232B44E9684163B6F66472C862
SHA-256:	F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48
SHA-512:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\4yGRcXEf.exe
File Type:	data
Category:	dropped
Size (bytes):	433680
Entropy (8bit):	**7.999538095926698**
Encrypted:	**true**
SSDEEP:	6144:lkuIpKmbvDHg+8RprJBRtt1pH6ZbnFowauxaeTg7hzzMK+gsCQX7SLB8KKV5B2Ny:FYbLHD8RJ3R12nUuQhzHAolSH
MD5:	7F0642B40D7F2EE4CF9D08601762F280
SHA1:	DB0A55E900FB8AB637F84815E8100DE9BA391810
SHA-256:	E6A52CF6101CD8A5B0B276BA0507AB1FA3203267B842C4534F28F37ADA40C02A
SHA-512:	108EB480E9AD78B3DD9783ED536B1406EB390F10CAFE0E95F26DA86D08B4E006FFFCE8EA389F87F4E6D92B0BFDA20EA8FD0BD6094D7E6EA773807D0ADBE1C 2E1
Malicious:	false
Reputation:	low
Preview:	.....O.....\8..5N..`S.]..[r.$*>.\.#v&..$.....Z.i..M.Mn5.@..@...3.R..Y...}>C.b....Z.....K..^.d...Z...K.#...dn$e ..XP.^.#.....V...dB.Kn.Y.c..-k....M.D...Q.S..R.X....._...Zz...#.= <.V.NHZq.h..ON..oq.:...,7H...../..Q..R.u6.."....<.`..z.5b($..9.CF.F1...o?.h.}....;Ay....kL}7...I.-.}..D&...C....%.J..+..1.5.a..Ih....s.....G..?..9^0e...p..FCvNt.e...B/...y.h.G.0..o,Q .2[.....e.P8.....yr...*..Q..*..../..S..m.....\.wA.a1.]...oW.....PY..h....f:.....Ss.....\.8...@R._A...M..X....V.f).]z..u{.z-....W...NaT+.&:...1.D../.7..\.S..z..!.....#..F.d.....*.m'..... .6.2....:H...bd]..._.....}.n.=...I.7%r.>...B.Q.K..q...Ex.6.6....P..^...i...Mx...;g...,t..fCd.\.b....e{.\...Y=4.....+..T....j}..|66g.s...z...Y.kTi..?Xy...5\...SO..W.U.3A.$.I..{.D...no.E..v.2 .:..a..hdhO..t.w.k..T|Po.....D?..mG.[.2.;....+...8.6.h!..w.3...w.o.....|....f.v.to.B.{`o..a.....f.cu.....?....."...u..EA...^)W..z..jtU{^.....5#....y.s.....e.l..&...%...

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.474968778910399
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	4yGRcXEf.exe
File size:	214528
MD5:	87e77797615466baa21cde3f7bb347f2
SHA1:	9cd228af2ea1f503fe76ed0ead2cfaab8ce7f08a

General	
SHA256:	d50a35f05df59b5b35e07dd204e5312629b3670b09da68 1c56f89c5aef8ff6b
SHA512:	cb88a2bfffec3ba7002e7d845e9d40f78285b822f17c24c2 1ec8c34ea488546466b4f1cddbed355f124dd8443004deb 34d02dce3a7a6e591c4f2590d1858c58c
SSDEEP:	6144:ELV6Bta6dtJmakIM55LTS/szPqJ6T8oXb4t:ELV6 BtpmkiY6hbc
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$.......PE..L....' .T.....................|........... ....@.. ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x41e792
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x54E927A1 [Sun Feb 22 00:49:37 2015 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x1e738	0x57	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x22000	0x17860	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x20000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x1c798	0x1c800	False	0.594512404057	data	6.59805753854	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.reloc	0x20000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x22000	0x17860	0x17a00	False	0.996569113757	data	7.99724840992	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x22058	0x17808	TIM image, Pixel at (43704,20504) Size=15294x49224		

Imports

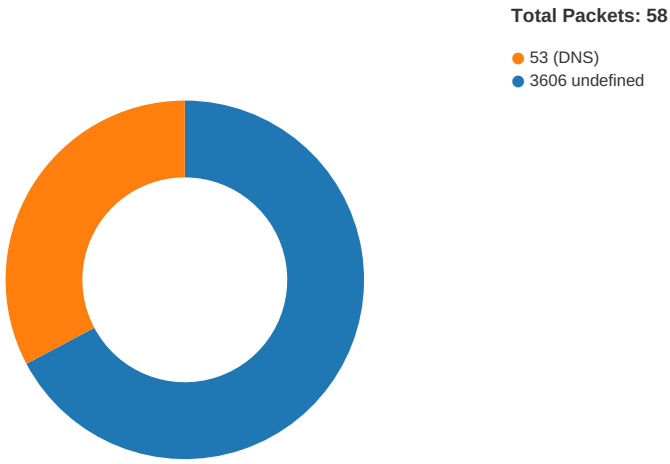
DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/23/20-14:49:14.930830	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49714	3606	192.168.2.5	79.134.225.77

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 14:49:14.832304001 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:14.898083925 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:14.898237944 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:14.930830002 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.015213966 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.022927999 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.088774920 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.109869957 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.211261034 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.263433933 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.263497114 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.263549089 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.263632059 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.263778925 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.263856888 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.328131914 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.328198910 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.328237057 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.328345060 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.328351974 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.328409910 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.329319000 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.329368114 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.329443932 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.329444885 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.329457998 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.329485893 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.329538107 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.390315056 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.390382051 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.390420914 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.390460014 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.390501976 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.390589952 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.390695095 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.390779972 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.390841961 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.391269922 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.391311884 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.391349077 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.391369104 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.391467094 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.391510010 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.391535044 CET	49714	3606	192.168.2.5	79.134.225.77

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 14:49:15.392153978 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.392196894 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.392245054 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.392297029 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.392355919 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.392370939 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.392442942 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.392908096 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.483490944 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.483525991 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.483629942 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.483668089 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.483756065 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.483819962 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.483884096 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.484009027 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.484545946 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.484606981 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.485165119 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.485222101 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.485270977 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.485311031 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.485420942 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.485438108 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.485502005 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.485538006 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.485591888 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.485657930 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.485774994 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.485824108 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.486059904 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.486135006 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.486186028 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.486571074 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.486596107 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.486639977 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.486654043 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.487369061 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.487413883 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.487497091 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.487495899 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.487580061 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.487642050 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.487652063 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.487720966 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.487739086 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.487804890 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.487816095 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.488360882 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.488415956 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.488440990 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.488468885 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.488501072 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.488557100 CET	49714	3606	192.168.2.5	79.134.225.77
Nov 23, 2020 14:49:15.488579035 CET	3606	49714	79.134.225.77	192.168.2.5
Nov 23, 2020 14:49:15.488635063 CET	49714	3606	192.168.2.5	79.134.225.77

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 14:49:07.519119978 CET	62176	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:07.546571016 CET	53	62176	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:08.520585060 CET	59596	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:08.548017979 CET	53	59596	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 23, 2020 14:49:09.325131893 CET	65296	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:09.352310896 CET	53	65296	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:10.111037970 CET	63183	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:10.146804094 CET	53	63183	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:14.593347073 CET	60151	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:14.794558048 CET	53	60151	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:21.864090919 CET	56969	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:21.891264915 CET	53	56969	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:26.181978941 CET	55161	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:26.209361076 CET	53	55161	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:28.627365112 CET	54757	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:28.654541969 CET	53	54757	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:32.446141005 CET	49992	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:32.483717918 CET	53	49992	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:32.656059980 CET	60075	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:32.683330059 CET	53	60075	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:34.956657887 CET	55016	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:34.983906031 CET	53	55016	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:50.141324043 CET	64345	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:50.185213089 CET	53	64345	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:58.106753111 CET	57128	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:58.133982897 CET	53	57128	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:58.191653967 CET	54791	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:58.196798086 CET	50463	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:58.219096899 CET	53	54791	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:58.246877909 CET	53	50463	8.8.8.8	192.168.2.5
Nov 23, 2020 14:49:59.724205971 CET	50394	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:49:59.751271963 CET	53	50394	8.8.8.8	192.168.2.5
Nov 23, 2020 14:50:02.246965885 CET	58530	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:50:02.290695906 CET	53	58530	8.8.8.8	192.168.2.5
Nov 23, 2020 14:50:02.919893980 CET	53813	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:50:02.957252026 CET	53	53813	8.8.8.8	192.168.2.5
Nov 23, 2020 14:50:34.158631086 CET	63732	53	192.168.2.5	8.8.8.8
Nov 23, 2020 14:50:34.186028957 CET	53	63732	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 23, 2020 14:49:14.593347073 CET	192.168.2.5	8.8.8.8	0x675a	Standard query (0)	poseidon99 .duckdns.org	A (IP address)	IN (0x0001)
Nov 23, 2020 14:50:02.246965885 CET	192.168.2.5	8.8.8.8	0x4a	Standard query (0)	g.msn.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 23, 2020 14:49:14.794558048 CET	8.8.8.8	192.168.2.5	0x675a	No error (0)	poseidon99 .duckdns.org		79.134.225.77	A (IP address)	IN (0x0001)
Nov 23, 2020 14:50:02.290695906 CET	8.8.8.8	192.168.2.5	0x4a	No error (0)	g.msn.com	g-msn-com-nsatc.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

System Behavior

Analysis Process: 4yGRcXEf.exe PID: 6748 Parent PID: 5708

General

Start time:	14:49:12
Start date:	23/11/2020
Path:	C:\Users\user\Desktop\4yGRcXEf.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\4yGRcXEf.exe'
Imagebase:	0x2b0000
File size:	214528 bytes
MD5 hash:	87E77797615466BAA21CDE3F7BB347F2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000000.224571570.00000000002B2000.00000002.00020000.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000000.224571570.00000000002B2000.00000002.00020000.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000000.224571570.00000000002B2000.00000002.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.233132403.0000000004534000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72B860AC	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	72B860AC	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	4D007A1	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	4D0089B	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	4D007A1	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	4D007A1	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	72B860AC	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	72B860AC	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	4D0089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4D0089B	CreateFileW
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	4D0089B	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\4yGRcXEf.exe:Zone.Identifier	success or wait	1	4D00B41	DeleteFileA

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	86 28 c8 ff 01 90 d8 48	.(.....H	success or wait	1	4D00A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	248	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 d5 c2 a4 ed f2 80 40 dc 33 8c a4 7b 0c cc 1c 67 72 76 2b 56 81 e7 f3 bf b9 42 19 0e 82 0d c5 eb 15 5d f3 50 8b f6 16 57 df 34 43 7d 75 4c 1e b2 de e3 a5 9f 66 d7 5a 23 80 7c 9b cc 91 a7 40 48 6b 47 10 1f c3 d0 b1 47 d7 d6 4f 2a 56 2e 15 0e d3 ab 8a d8 9f 99 c3 dc e8 70 7a ba ae a5 8f 22 84 0a 07 be 72 b5 c3 10 77 26 26 7c ed ce 63 bb d0 33 7d 7e 84 eb d7 1d 9d 7e b6 cb b6 ff 6f 73 f4 b2 66 d6 05 e9 12 d4 e2 ca 34 12 de 31 9f 67 4a de 27 d7 64 22 d1 4c ba 0b cc 41 90 74 b3 c3 87 d5 46 f9 7b ca c8 ab 14 80 43 0c 7c 26 aa 77	Gj.h\.3..A...5.x..&...i+...c(1 .P..P.cLT....A.b.....4h...t .+..Z\.. .i.....@.3..{...grv +V.....B.....].P...W.4C}uL.. ....f.Z#.|....@HkG.....G..O* V.....pz....".....r...w&&| ..c..3}~.....~....os..f..... 4..1.gJ.'.d".L...A.t....F.{... ..C.|&.w	success or wait	1	4D00A53	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	unknown	433680	f5 ec cd 01 d2 e1 d2 c2 10 4f 02 de b7 c5 8d 0e b8 e2 19 5c 38 e3 e0 35 4e a8 a9 60 53 d0 5d ea fb 5b 72 f8 24 2a 3e c2 5c 94 23 76 26 f9 84 24 a5 d6 19 d8 c7 df f6 5a ef bd 69 f7 86 4d e9 4d 6e 35 1d 40 e8 d2 40 bd 10 97 33 fa 52 d1 b7 cb 59 d9 ac b5 d9 7d 3e 43 1e 62 92 ed 0a 8b 5a bc da c3 e6 d4 08 cb e5 4b 98 ac 5e ac 64 d2 e7 fd 5a ef fe 13 4b a8 23 af e7 1b 64 6e 24 65 20 0d 9e 58 50 02 5e fc 23 cc d5 bd ae 8a ea 17 d0 56 95 c5 12 64 42 ad 4b 6e e4 59 af 63 0b e6 2d 6b c5 07 18 d2 89 4d 0c 44 d0 8a 0a ac 51 de 53 87 bc 52 ca ad 58 8d 8f 0e e2 17 05 ec 19 f0 1a 5f f4 b2 bd 5a 7a b1 e5 b8 d0 23 08 3d 3c 08 56 e3 4e 48 5a 71 cc b9 68 99 13 4f 4e a3 dd 6f 71 c1 3a c5 18 1f 2c 37 48 da 07 f3 d0 f0 90 e6 2f fc ba 51 c3 d0 bf 52 1b 75 36 19 dd 81 22 b2 c4	.....O.....\8..5N..`S.]..[r.$*>.\.#v&..$.....Z..i..M.Mn5.@..@...3.R...Y....}>C.b....Z.....K..^.d...Z...K.#...dn$e ..XP.^.#.....V...dB.Kn.Y.c..-k.....M.D....Q.S..R..X....._...Zz....#.=<.V.NHZq..h..ON..oq.:...,7H...../..Q...R.u6.."..	success or wait	1	4D00A53	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	unknown	40	39 69 48 cc 1a df 85 7d 5a d7 8d 34 00 a8 66 0d 7e 61 d3 f8 a3 01 06 96 0c a9 7e ba 7e 86 90 d9 e5 05 8d ca 33 e7 55 0b	9iH....}Z..4..f.~a.....~.~.....3.U.	success or wait	1	4D00A53	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	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB8738	ReadFile
C:\Users\user\Desktop\4yGRcXEf.exe	unknown	4096	success or wait	1	72C5BF06	unknown
C:\Users\user\Desktop\4yGRcXEf.exe	unknown	512	success or wait	1	72C5BF06	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	72BB5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4D00A53	ReadFile

Disassembly

Code Analysis