ID: 403331
Sample Name:
f908098a_by_Libranalysis
Cookbook: default.jbs
Time: 03:39:11
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

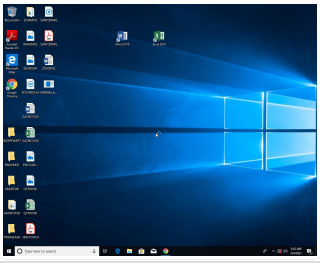
Analysis Report f908098a_by_Libranalysis

Overview

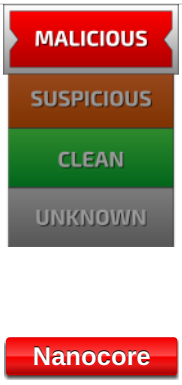
General Information

Sample Name:	f908098a_by_Libranalysis (renamed file extension from none to exe)
Analysis ID:	403331
MD5:	f908098af6b73a5..
SHA1:	7c92b17c6e2ede..
SHA256:	aeb4339ff4e4d6f…
Infos:	

Most interesting Screenshot:



Detection



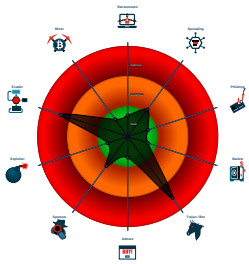
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- .NET source code contains very larg…
- C2 URLs / IPs found in malware con…
- Hides threads from debuggers
- Machine Learning detection for samp…
- Potential time zone aware malware
- Binary contains a suspicious time st…
- Contains capabilities to detect virtua…

Classification



Startup

- **System is w10x64**
- f908098a_by_Libranalysis.exe (PID: 6652 cmdline: 'C:\Users\user\Desktop\f908098a_by_Libranalysis.exe' MD5: F908098AF6B73A5EA4081A3474030196)
  - backgroundTaskHost.exe (PID: 6724 cmdline: 'C:\Windows\system32\backgroundTaskHost.exe' -ServerName:App.AppXmtcan0h2tfbfy7k9kn8hbxb6dmzz1zh0.mca MD5: B7FC4A29431D4F795BBAB1FB182B759A)
  - cmd.exe (PID: 6948 cmdline: 'C:\Windows\System32\cmd.exe' /c timeout 1 MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - timeout.exe (PID: 7004 cmdline: timeout 1 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
  - f908098a_by_Libranalysis.exe (PID: 7072 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 7088 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - taskhostw.exe (PID: 7104 cmdline: taskhostw.exe None MD5: CE95E236FC9FE2D6F16C926C75B18BAF)
  - svchost.exe (PID: 7116 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - f908098a_by_Libranalysis.exe (PID: 7124 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 2912 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 4824 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6208 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6388 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6340 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6352 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 5936 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 5920 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 5924 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 5964 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 5968 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 5660 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6168 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - svchost.exe (PID: 6596 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - f908098a_by_Libranalysis.exe (PID: 6660 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6268 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6400 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6412 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6508 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6692 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 7020 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 7016 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 6984 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 7036 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
  - f908098a_by_Libranalysis.exe (PID: 4876 cmdline: C:\Users\user\Desktop\f908098a_by_Libranalysis.exe MD5: F908098AF6B73A5EA4081A3474030196)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "Version": "1.2.2.0",
  "Mutex": "b3bfe601-8f28-4397-a972-90d172cf",
  "Group": "Default",
  "Domain1": "fedex.itemdb.com",
  "Domain2": "uspslabel.itemdb.com",
  "Port": 1090,
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000002.746272772.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000001F.00000002.746272772.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000001F.00000002.746272772.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
0000000E.00000002.708373051.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000E.00000002.708373051.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 100 entries				

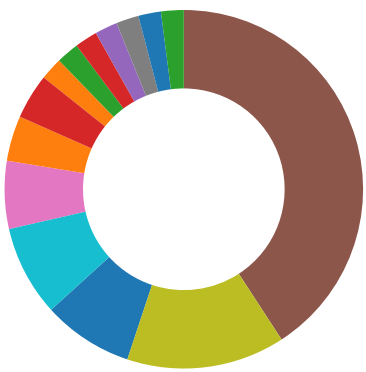
Unpacked PEs

Source	Rule	Description	Author	Strings
22.2.f908098a_by_Libranalysis.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
22.2.f908098a_by_Libranalysis.exe.400000.0.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xff05:$x1: NanoCore Client.exe • 0x1018d:$x2: NanoCore.ClientPluginHost • 0x117c6:$s1: PluginCommand • 0x117ba:$s2: FileCommand • 0x1266b:$s3: PipeExists • 0x18422:$s4: PipeCreated • 0x101b7:$s5: IClientLoggingHost
22.2.f908098a_by_Libranalysis.exe.400000.0.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
22.2.f908098a_by_Libranalysis.exe.400000.0.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:$j: #=q
19.2.f908098a_by_Libranalysis.exe.400000.0.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 71 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

- AV Detection
- Compliance
- Spreading
- 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
- Stealing of Sensitive Information
- Remote Access Functionality

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

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:

.NET source code contains potential unpacker

Malware Analysis System Evasion:

Potential time zone aware malware

Anti Debugging:

Hides threads from debuggers

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

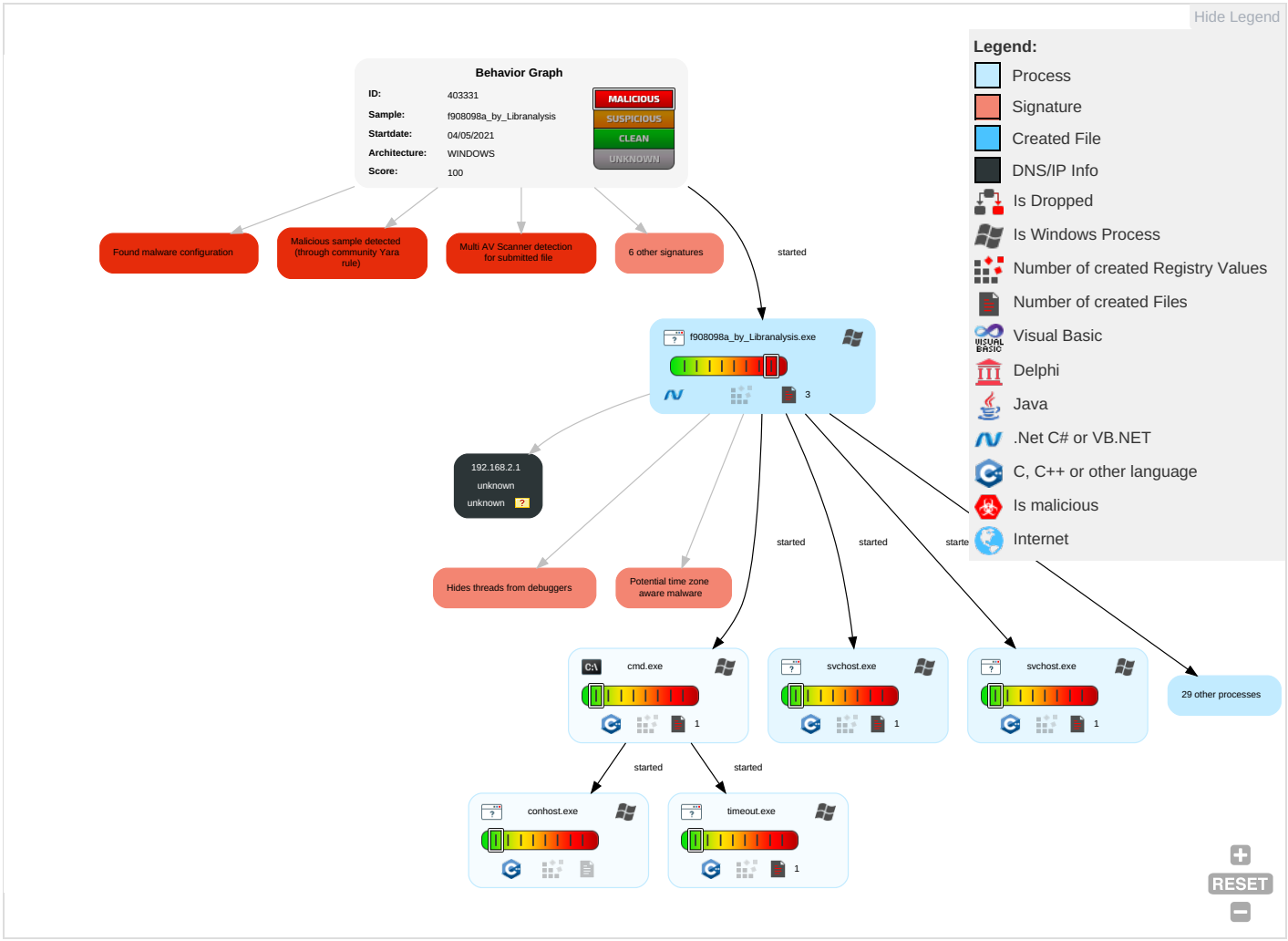
Yara detected Nanocore RAT

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	Path Interception	Process Injection 1 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Remote Access Software 1	Eavesdrop o Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 1 1	Security Account Manager	Virtualization/Sandbox Evasion 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	File and Directory Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Timestomp 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

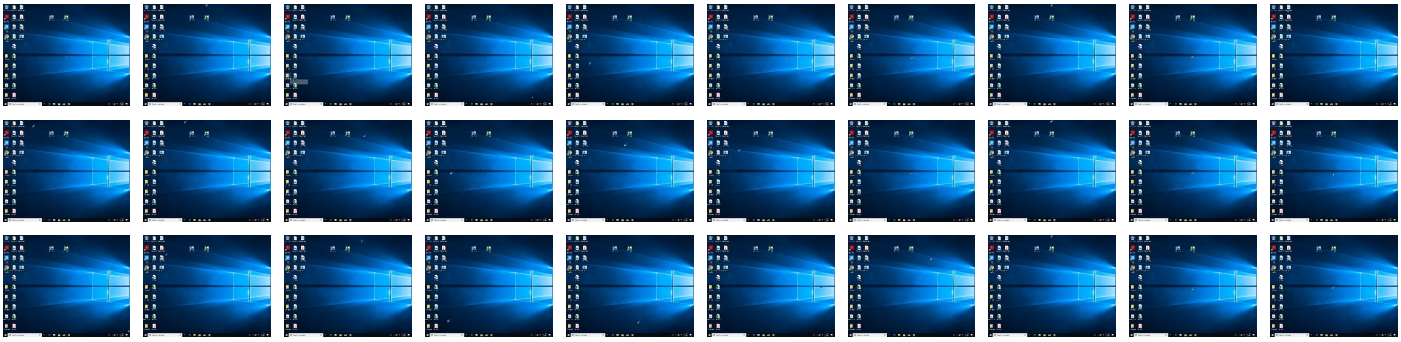
Behavior Graph

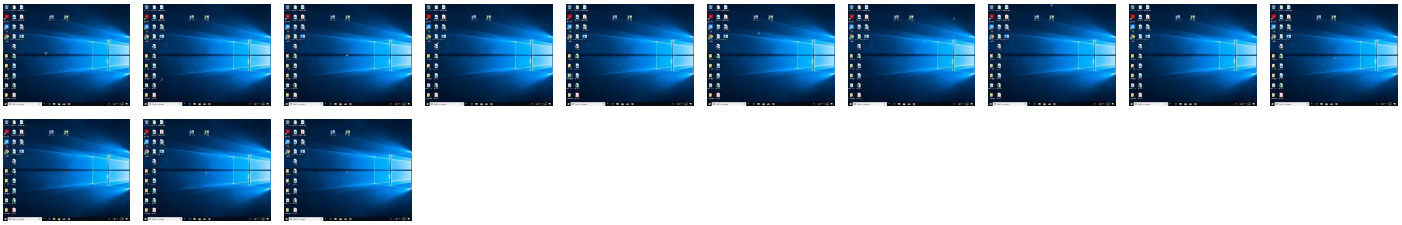


Screenshots

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
f908098a_by_Libranalysis.exe	30%	Virustotal		Browse
f908098a_by_Libranalysis.exe	32%	ReversingLabs		
f908098a_by_Libranalysis.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File

Source	Detection	Scanner	Label	Link	Download
18.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
37.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
17.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
19.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
28.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
24.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
11.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
29.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
13.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
8.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
39.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
16.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
21.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
31.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
15.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
14.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
33.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File
12.2.f908098a_by_Libranalysis.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1108376		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
fedex.itemdb.com	3%	Virustotal		Browse
fedex.itemdb.com	0%	Avira URL Cloud	safe	
uspslabel.itemdb.com	1%	Virustotal		Browse
uspslabel.itemdb.com	0%	Avira URL Cloud	safe	

Domains and IPs

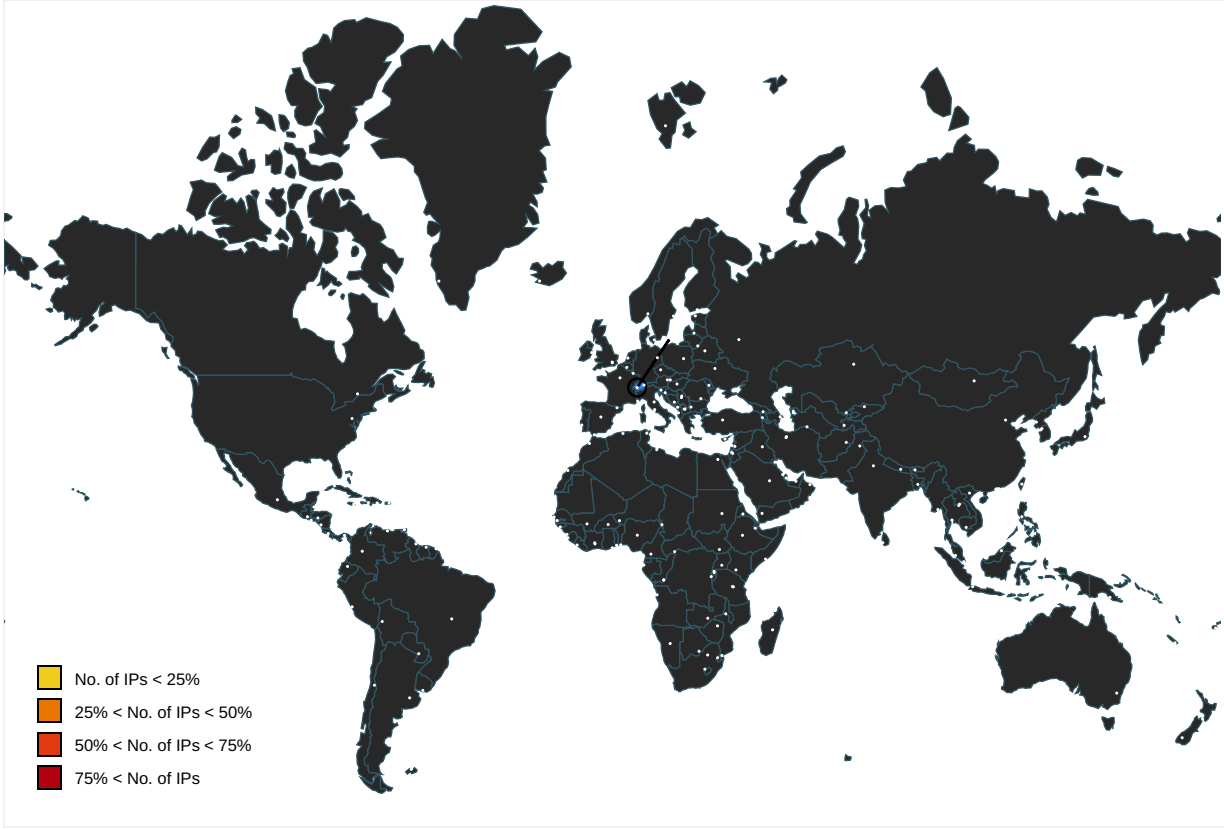
Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
fedex.itemdb.com	true	• 3%, Virustotal, Browse • Avira URL Cloud: safe	unknown
uspslabel.itemdb.com	true	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403331
Start date:	04.05.2021
Start time:	03:39:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	f908098a_by_Libranalysis (renamed file extension from none to 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:	40
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@261/0@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
Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtReadVirtualMemory calls found. • Report size getting too big, too many NtWriteVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.5846346250292926
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 50.01% • Win32 Executable (generic) a (10002005/4) 49.97% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	f908098a_by_Libranalysis.exe
File size:	2311168
MD5:	f908098af6b73a5ea4081a3474030196
SHA1:	7c92b17c6e2ede3e3bee94c41603795c93d53c89
SHA256:	aeb4339ff4e4d6f8249236e1280111324d84920c23a169cffc67577ab9f69217
SHA512:	de7957ec6b9189692c239e7198736259f755f5e2d7b881cd5f8c56aff8755686e0ee6bd7ac1cf147474c31a8994088fbefd4f54a576316c42c8020e6df4eb9f1
SSDEEP:	1536:6cvkyC4QOoyJ+e6LlKK6Prm6P/T6jAnJ6RIB6P9J/e6LoB7/s6/nYBew18hZEMGd:Bm
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...P.;....."...0..:#.....~Y#.. ...`#...@.. .....#.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x63597e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xD93B9850 [Thu Jun 28 10:11:28 2085 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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

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

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
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	0x235930	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x236000	0x588	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x238000	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	0x233984	0x233a00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x236000	0x588	0x600	False	0.412760416667	data	4.01111930109	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x238000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x2360a0	0x2fc	data		

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x23639c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	first.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	first
ProductVersion	1.0.0.0
FileDescription	first
OriginalFilename	first.exe

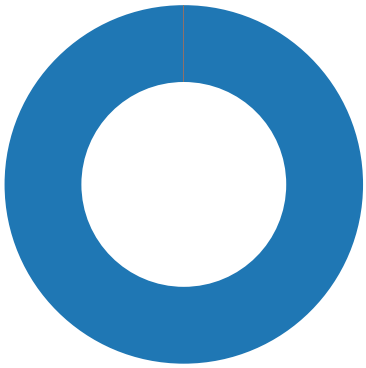
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



- f908098a_by_Libranalysis.exe
- backgroundTaskHost.exe
- cmd.exe
- conhost.exe
- timeout.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- taskhostw.exe
- svchost.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- svchost.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe
- f908098a_by_Libranalysis.exe

f908098a_by_Libranalysis.exe
f908098a_by_Libranalysis.exe
f908098a_by_Libranalysis.exe

Click to jump to process

System Behavior

Analysis Process: f908098a_by_Libranalysis.exe PID: 6652 Parent PID: 5812

General

Start time:	03:40:11
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\f908098a_by_Libranalysis.exe'
Imagebase:	0xd50000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000000.00000003.845726341.00000000071B2000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.845726341.00000000071B2000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.845726341.00000000071B2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.805194004.0000000004ACD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.805194004.0000000004ACD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.805194004.0000000004ACD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.891871365.0000000004ACD000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.891871365.0000000004ACD000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.891871365.0000000004ACD000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.805655388.0000000005206000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.805655388.0000000005206000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.805655388.0000000005206000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.858964589.0000000004B49000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.858964589.0000000004B49000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.858964589.0000000004B49000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.818065172.0000000007C37000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.818065172.0000000007C37000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.818065172.0000000007C37000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000000.00000003.814590016.0000000007237000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000003.814590016.0000000007237000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000003.814590016.0000000007237000.00000004.00000001.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	6D17CF06	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	6D17CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D155705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D15CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D0B03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D0B03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D155705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6BFC1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6BFC1B4F	ReadFile

Analysis Process: backgroundTaskHost.exe PID: 6724 Parent PID: 800

General

Start time:	03:40:13
Start date:	04/05/2021
Path:	C:\Windows\System32\backgroundTaskHost.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\backgroundTaskHost.exe' -ServerName:App.AppXmtcan0h2tfbfy7k 9kn8hbxb6dmzz1zh0.mca
Imagebase:	0x7ff732050000
File size:	19352 bytes
MD5 hash:	B7FC4A29431D4F795BBAB1FB182B759A
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: cmd.exe PID: 6948 Parent PID: 6652

General

Start time:	03:40:18
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe

Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\cmd.exe' /c timeout 1
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6964 Parent PID: 6948

General

Start time:	03:40:18
Start date:	04/05/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 7004 Parent PID: 6948

General

Start time:	03:40:19
Start date:	04/05/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 1
Imagebase:	0xb70000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: f908098a_by_Libranalysis.exe PID: 7072 Parent PID: 6652

General

Start time:	03:40:22
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x2a0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 7088 Parent PID: 6652

General

Start time:	03:40:23
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x6c0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000008.00000002.699198660.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000008.00000002.699198660.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000008.00000002.699198660.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: taskhostw.exe PID: 7104 Parent PID: 968

General

Start time:	03:40:23
Start date:	04/05/2021
Path:	C:\Windows\System32\taskhostw.exe
Wow64 process (32bit):	false
Commandline:	taskhostw.exe None
Imagebase:	0x7ff73c340000
File size:	87904 bytes
MD5 hash:	CE95E236FC9FE2D6F16C926C75B18BAF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: svchost.exe PID: 7116 Parent PID: 568

General

Start time:	03:40:23
Start date:	04/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: f908098a_by_Libranalysis.exe PID: 7124 Parent PID: 6652

General

Start time:	03:40:24
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xf90000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 0000000B.00000002.701491869.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000B.00000002.701491869.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000B.00000002.701491869.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 2912 Parent PID: 6652

General

Start time:	03:40:25
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xf80000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 0000000C.00000002.703895880.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000C.00000002.703895880.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000C.00000002.703895880.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 4824 Parent PID: 6652

General

Start time:	03:40:26
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xea0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 0000000D.00000002.706079579.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.706079579.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.706079579.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6208 Parent PID: 6652

General

Start time:	03:40:27
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xe30000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 0000000E.00000002.708373051.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000E.00000002.708373051.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000E.00000002.708373051.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6388 Parent PID: 6652

General

Start time:	03:40:28
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xb80000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 0000000F.00000002.711316230.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.711316230.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.711316230.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6340 Parent PID: 6652

General

Start time:	03:40:29
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x600000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000010.00000002.714383017.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000010.00000002.714383017.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000010.00000002.714383017.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6352 Parent PID: 6652

General

Start time:	03:40:31
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xa70000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000011.00000002.716772680.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000011.00000002.716772680.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000011.00000002.716772680.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 5936 Parent PID: 6652

General

Start time:	03:40:32
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x980000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000012.00000002.718926424.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000012.00000002.718926424.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000012.00000002.718926424.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 5920 Parent PID: 6652

General

Start time:	03:40:33
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xd30000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000013.00000002.721358453.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000013.00000002.721358453.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000013.00000002.721358453.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 5924 Parent PID: 6652

General

Start time:	03:40:34
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x150000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 5964 Parent PID: 6652

General

Start time:	03:40:35
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x760000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000015.00000002.725332154.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000015.00000002.725332154.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000015.00000002.725332154.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 5968 Parent PID: 6652

General

Start time:	03:40:36
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xcd0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000016.00000002.727791408.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000016.00000002.727791408.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000016.00000002.727791408.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 5660 Parent PID: 6652

General

Start time:	03:40:37
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x470000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000018.00000002.730062781.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.730062781.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.730062781.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6168 Parent PID: 6652

General

Start time:	03:40:38
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x3c0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: svchost.exe PID: 6596 Parent PID: 568

General

Start time:	03:40:38
Start date:	04/05/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: f908098a_by_Libranalysis.exe PID: 6660 Parent PID: 6652

General

Start time:	03:40:39
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x300000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6268 Parent PID: 6652

General

Start time:	03:40:40
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xce0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 0000001C.00000002.736073940.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001C.00000002.736073940.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001C.00000002.736073940.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6400 Parent PID: 6652

General

Start time:	03:40:41
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xc90000

File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 0000001D.00000002.738600817.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001D.00000002.738600817.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001D.00000002.738600817.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6412 Parent PID: 6652

General

Start time:	03:40:42
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x310000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: f908098a_by_Libranalysis.exe PID: 6508 Parent PID: 6652

General

Start time:	03:40:45
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xbf0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 0000001F.00000002.746272772.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000001F.00000002.746272772.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000001F.00000002.746272772.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: f908098a_by_Libranalysis.exe PID: 6692 Parent PID: 6652

General

Start time:	03:40:46
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xf50000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000021.00000002.748683152.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000021.00000002.748683152.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000021.00000002.748683152.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: f908098a_by_Libranalysis.exe PID: 7020 Parent PID: 6652

General

Start time:	03:40:47
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x1b0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: f908098a_by_Libranalysis.exe PID: 7016 Parent PID: 6652

General

Start time:	03:40:48
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xc0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: f908098a_by_Libranalysis.exe PID: 6984 Parent PID: 6652

General

Start time:	03:40:49
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe

Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xf20000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000025.00000002.757220871.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000025.00000002.757220871.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000025.00000002.757220871.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: f908098a_by_Libranalysis.exe PID: 7036 Parent PID: 6652

General

Start time:	03:40:51
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0x2b0000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: f908098a_by_Libranalysis.exe PID: 4876 Parent PID: 6652

General

Start time:	03:40:52
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\f908098a_by_Libranalysis.exe
Imagebase:	0xe30000
File size:	2311168 bytes
MD5 hash:	F908098AF6B73A5EA4081A3474030196
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: 00000027.00000002.762072262.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000027.00000002.762072262.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000027.00000002.762072262.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Disassembly

Code Analysis