

JOeSandbox Cloud BASIC



ID: 339358

Sample Name: Invoice# 77-
84993-84929.exe

Cookbook: default.jbs

Time: 21:36:32

Date: 13/01/2021

Version: 31.0.0 Red Diamond

Table of Contents

Table of Contents	2
Analysis Report Invoice# 77-84993-84929.exe	4
Overview	4
General Information	4
Detection	4
Signatures	4
Classification	4
Startup	4
Malware Configuration	4
Yara Overview	4
Memory Dumps	4
Unpacked PEs	5
Sigma Overview	5
System Summary:	5
Signature Overview	6
AV Detection:	6
E-Banking Fraud:	6
System Summary:	6
Data Obfuscation:	6
Hooking and other Techniques for Hiding and Protection:	6
Malware Analysis System Evasion:	6
Stealing of Sensitive Information:	6
Remote Access Functionality:	6
Mitre Att&ck Matrix	7
Behavior Graph	7
Screenshots	8
Thumbnails	8
Antivirus, Machine Learning and Genetic Malware Detection	9
Initial Sample	9
Dropped Files	9
Unpacked PE Files	9
Domains	9
URLs	9
Domains and IPs	10
Contacted Domains	10
Contacted IPs	10
Public	10
Private	10
General Information	10
Simulations	11
Behavior and APIs	11
Joe Sandbox View / Context	11
IPs	11
Domains	11
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	12
Static File Info	12
General	12
File Icon	13
Static PE Info	13
General	13
Entrypoint Preview	13
Data Directories	15
Sections	15

Resources	15
Imports	15
Version Infos	15
Network Behavior	16
Code Manipulations	16
Statistics	16
Behavior	16
System Behavior	16
Analysis Process: Invoice# 77-84993-84929.exe PID: 6104 Parent PID: 5864	16
General	16
File Activities	16
File Created	16
File Written	17
File Read	17
Analysis Process: Invoice# 77-84993-84929.exe PID: 5732 Parent PID: 6104	18
General	18
File Activities	20
File Created	20
File Deleted	20
File Written	20
File Read	20
Disassembly	20
Code Analysis	21

Analysis Report Invoice# 77-84993-84929.exe

Overview

General Information

Sample Name:

Invoice# 77-84993-84929.exe

Analysis ID:

339358

MD5:

3beaa725263104..

SHA1:

da267ad7c11acb..

SHA256:

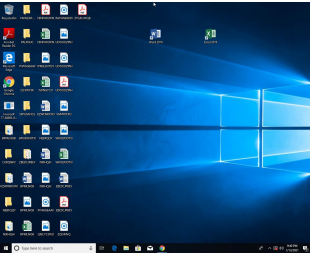
eba0abe9461df84.

Tags:

exe

NanoCore

Most interesting Screenshot:



Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Nanocore

Score:

100

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Detected Nanocore Rat

Malicious sample detected (through ...

Multi AV Scanner detection for subm...

Sigma detected: NanoCore

Yara detected AntiVM_3

Yara detected Nanocore RAT

.NET source code contains potentia...

Binary contains a suspicious time st...

Hides that the sample has been dow...

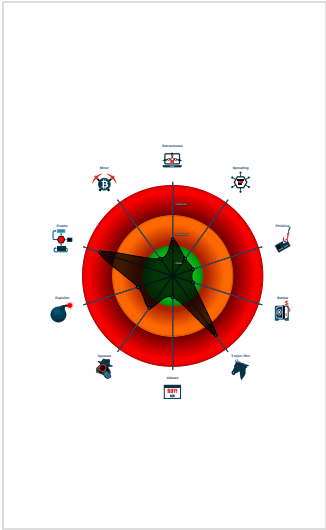
Initial sample is a PE file and has a ...

Machine Learning detection for samp...

Tries to detect sandboxes and other...

Contains long sleeps (>= 3 min)

Classification



Startup

System is w10x64

Invoice# 77-84993-84929.exe

(PID: 6104 cmdline: 'C:\Users\user\Desktop\Invoice# 77-84993-84929.exe' MD5: 3BEAA725263104D4638EB877A7D0B37D)

Invoice# 77-84993-84929.exe

(PID: 5732 cmdline: {path} MD5: 3BEAA725263104D4638EB877A7D0B37D)

cleanup

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.699728992.0000000006DE0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x1aa7d:\$x1: NanoCore.ClientPluginHost 0x1aa6a:\$x2: IClientNetworkHost 0x19142:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcfp8PZGe
00000001.00000002.699728992.0000000006DE0000.00000004.00000001.sdmp	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0x19983:\$x1: NanoCore Client.exe 0x1aa7d:\$x2: NanoCore.ClientPluginHost 0x19120:\$s1: PluginCommand 0x19108:\$s2: FileCommand 0x1a88b:\$s3: PipeExists 0x190d8:\$s4: PipeCreated 0x1aa57:\$s5: IClientLoggingHost
00000001.00000002.699728992.0000000006DE0000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000001.00000002.699728992.0000000006DE 0000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@technarchy.net>	• 0x19536:\$a: NanoCore • 0x19983:\$a: NanoCore • 0x19e84:\$a: NanoCore • 0x1a974:\$a: NanoCore • 0x1aa7d:\$a: NanoCore • 0x19e8d:\$b: ClientPlugin • 0x1aa86:\$b: ClientPlugin • 0x18f48:\$c: ProjectData • 0x332cd:\$c: ProjectData • 0x1a295:\$d: DESCrypto • 0x1991a:\$e: KeepAlive • 0x1927a:\$g: LogClientMessage • 0x190e4:\$i: get_Connected • 0xfc25:\$j: #=q • 0xfc76:\$j: #=q • 0xfcba:\$j: #=q • 0xfdd5:\$j: #=q • 0xfe3a:\$j: #=q • 0xfe9f:\$j: #=q • 0xfeef:\$j: #=q • 0xff33:\$j: #=q
00000001.00000002.699774289.0000000006E2 0000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1a82d:\$x1: NanoCore.ClientPluginHost • 0x1a81a:\$x2: IClientNetworkHost • 0x18ef2:\$x3: #=qjgz7ljmpp0J7FvL9dm8ctJlLdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
Click to see the 52 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Invoice# 77-84993-84929.exe.6c90000.6.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x1980d:\$x1: NanoCore.ClientPluginHost 0x197fa:\$x2: IClientNetworkHost 0x17ed2:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
1.2.Invoice# 77-84993-84929.exe.6c90000.6.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	0x18713:\$x1: NanoCore.Client.exe 0x1980d:\$x2: NanoCore.ClientPluginHost 0x17eb0:\$s1: PluginCommand 0x17e98:\$s2: FileCommand 0x1961b:\$s3: PipeExists 0x17e68:\$s4: PipeCreated 0x197e7:\$s5: IClientLoggingHost
1.2.Invoice# 77-84993-84929.exe.6c90000.6.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
1.2.Invoice# 77-84993-84929.exe.6c90000.6.unpack	NanoCore	unknown	Kevin Breen <kevin@technarchy.net>	0x182c6:\$a: NanoCore 0x18713:\$a: NanoCore 0x18c14:\$a: NanoCore 0x19704:\$a: NanoCore 0x1980d:\$a: NanoCore 0x18c1d:\$b: ClientPlugin 0x19816:\$b: ClientPlugin 0x17cd8:\$c: ProjectData 0x3205d:\$c: ProjectData 0x3487d:\$c: ProjectData 0x36ce0:\$c: ProjectData 0x391a5:\$c: ProjectData 0x3bb38:\$c: ProjectData 0x3e599:\$c: ProjectData 0x19025:\$d: DESCrypto 0x186aa:\$e: KeepAlive 0x1800a:\$g: LogClientMessage 0x17e74:\$i: get_Connected 0xe9b5:\$j: #=q 0xea06:\$j: #=q 0xea4a:\$j: #=q
1.2.Invoice# 77-84993-84929.exe.6da0000.10.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	0x18ecd:\$x1: NanoCore.ClientPluginHost 0x18eba:\$x2: IClientNetworkHost 0x17592:\$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Click to see the 83 entries

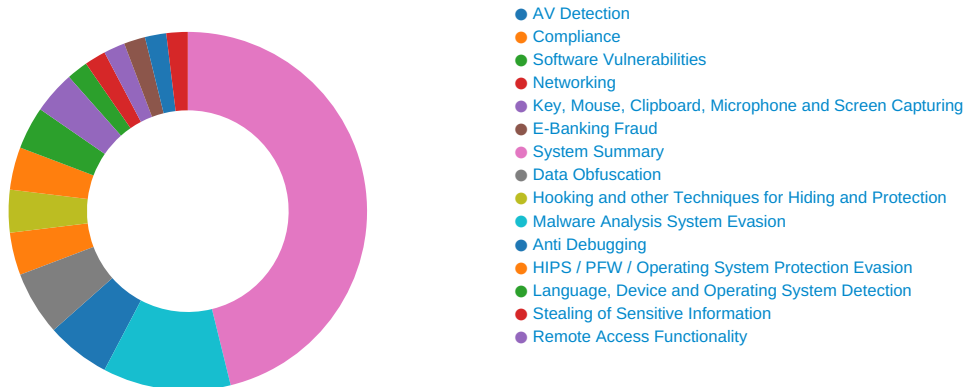
Sigma Overview

System Summary:



Sigma detected: NanoCore

Signature Overview



Click to jump to signature section

AV Detection:



Multi AV Scanner detection for submitted file

Yara detected Nanocore RAT

Machine Learning detection for sample

E-Banking Fraud:



Yara detected Nanocore RAT

System Summary:



Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:



.NET source code contains potential unpacker

Binary contains a suspicious time stamp

Hooking and other Techniques for Hiding and Protection:



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

Malware Analysis System Evasion:



Yara detected AntiVM_3

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

Stealing of Sensitive Information:



Yara detected Nanocore RAT

Remote Access Functionality:

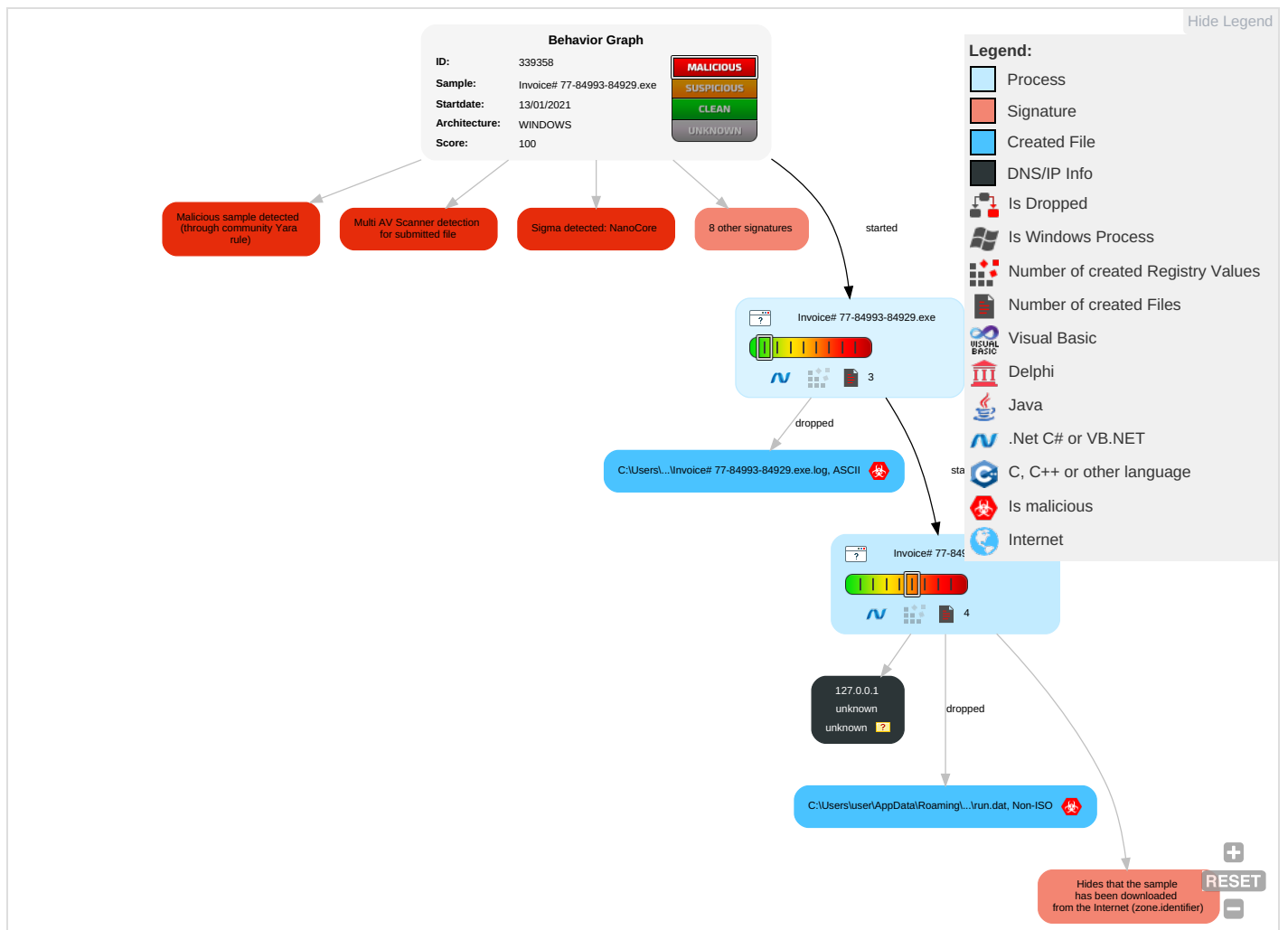


Detected Nanocore Rat

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 2	Masquerading 1	Input Capture 1	Security Software Discovery 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
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	Archive Collected Data 1	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit SS7 Redirect Phone Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	System Information Discovery 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	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 Point
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Timestomp 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols

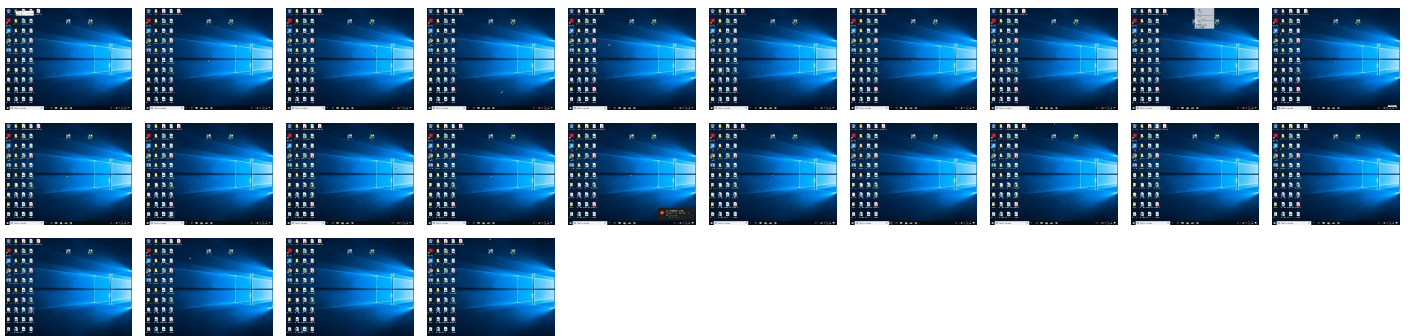
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Invoice# 77-84993-84929.exe	28%	ReversingLabs	Win32.PUA.Wacapew	
Invoice# 77-84993-84929.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

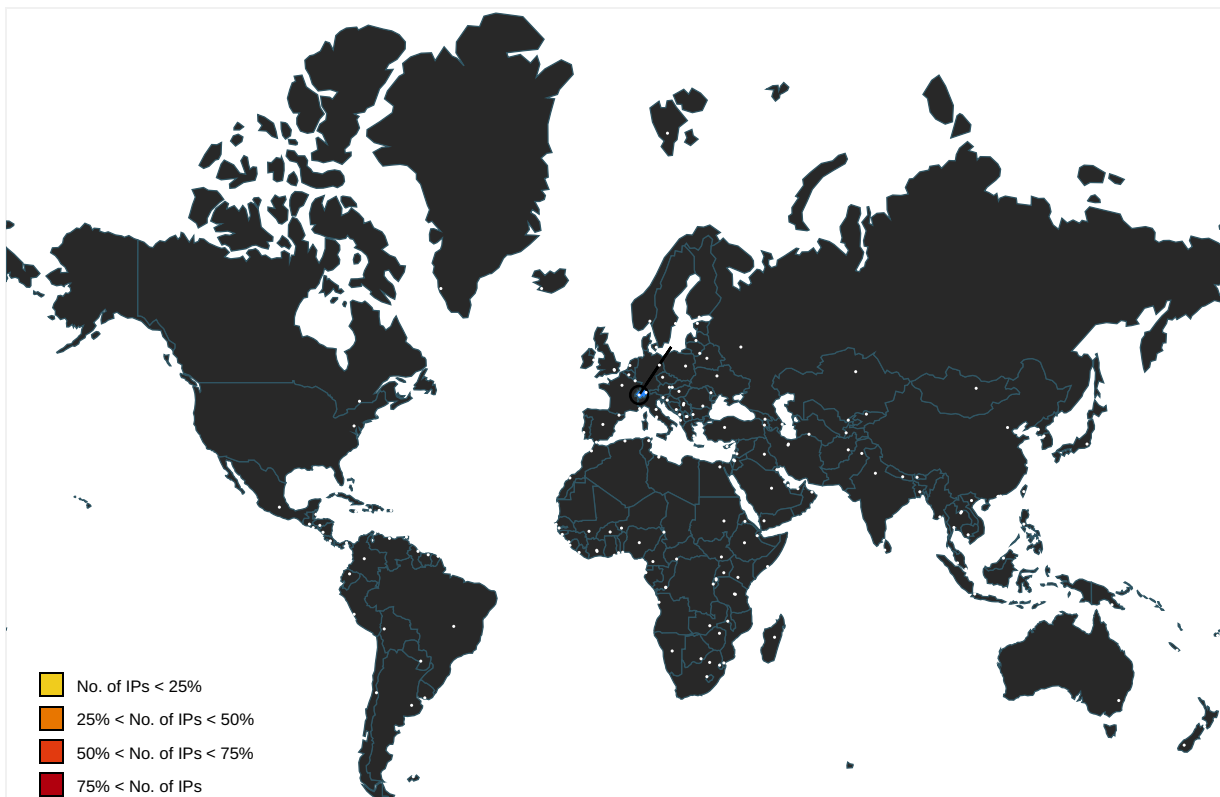
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
----	--------	---------	------	-----	----------	-----------

Private

IP

127.0.0.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	339358
Start date:	13.01.2021
Start time:	21:36:32
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Invoice# 77-84993-84929.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:	7

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@3/2@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 79.9% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, svchost.exe • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

Time	Type	Description
21:37:27	API Interceptor	1124x Sleep call for process: Invoice# 77-84993-84929.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice# 77-84993-84929.exe.log		
Process:	C:\Users\user\Desktop\Invoice# 77-84993-84929.exe	
File Type:	ASCII text, with CRLF line terminators	
Category:	dropped	
Size (bytes):	1216	
Entropy (8bit):	5.355304211458859	
Encrypted:	false	
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr	
MD5:	FED34146BF2F2FA59DCF8702FCC8232E	
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A	
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C	
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F6	
Malicious:	true	
Reputation:	high, very likely benign file	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21	

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat		
Process:	C:\Users\user\Desktop\Invoice# 77-84993-84929.exe	
File Type:	Non-ISO extended-ASCII text, with no line terminators	
Category:	dropped	
Size (bytes):	8	
Entropy (8bit):	3.0	
Encrypted:	false	
SSDEEP:	3:2/l:ql	
MD5:	904C75C757951861A0708BE11E7058FB	
SHA1:	8835D363C38767D84A5A3E2483CD1B94EE7FF0CD	
SHA-256:	86B9242C9DB4D22310489A0E372733E9E029A08A05E219ACC1BDE7CC02E6809E	
SHA-512:	EBAC3B8031EF52CFBDF971D28B4C8CEE82B12F64CE0193F3DA3E989DF946D290EC9F90097B6CC75CB582C441E4D65F8CA73A517EE03EC3C14200F6A60DF20F	
Malicious:	true	
Reputation:	low	
Preview:	.O?.N..H	

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.949599343543474
TrID:	- Win32 Executable (generic) Net Framework (10011505/4) 49.80% - Win32 Executable (generic) a (10002005/4) 49.75% - Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% - Windows Screen Saver (13104/52) 0.07% - Generic Win/DOS Executable (2004/3) 0.01%
File name:	Invoice# 77-84993-84929.exe
File size:	1082880
MD5:	3beaa725263104d4638eb877a7d0b37d
SHA1:	da267ad7c11acb864db25a561fea1e2cc3663fd0
SHA256:	eba0abe9461df84c76949df2d559f66b0379cbdbd430f8db884c55d0aa469980
SHA512:	efa1dfea9a15b9cb8c15bed2d510d0c8f879ba2ccf377e0c134d0f0c9047feabc2c17f20bfcf089f33c237391258bf020bb9041308d573a63ca63415e2f459e7

General	
SSDEEP:	24576:pVTN1bAVAAo+sZ5Ox7NJEAbUfl0u/r3qEO5CL TvaskuDKUZ:HNG6o+Py+25C/asxJZ
File Content Preview:	MZ.....@.....!..L!Th is program cannot be run in DOS mode...\$.PE..L.. B3.....0..@.. ...@.....

File Icon	
Icon Hash:	00828e8e8686b000

Static PE Info

General	
Entrypoint:	0x509b8e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xE7183342 [Mon Nov 10 02:34:42 2092 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

[illegible]

Instruction

[illegible]

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x109b3c	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x10a000	0x5d4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x10c000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x109b20	0x1c	.text
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	0x107b94	0x107c00	False	0.952498333827	data	7.95337627624	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x10a000	0x5d4	0x600	False	0.427083333333	data	4.14249009427	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x10c000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x10a090	0x344	data		
RT_MANIFEST	0x10a3e4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscorlib.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2019
Assembly Version	1.0.0.0
InternalName	bB.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	MultiUserParentalControl
ProductVersion	1.0.0.0
FileDescription	MultiUserParentalControl
OriginalFilename	bB.exe

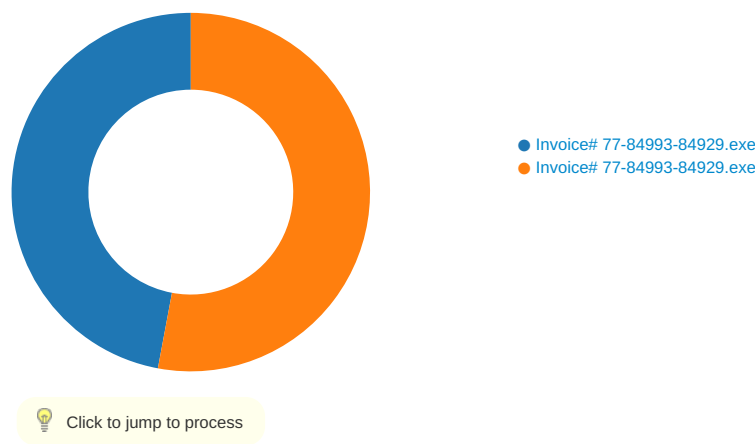
Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: Invoice# 77-84993-84929.exe PID: 6104 Parent PID: 5864

General

Start time:	21:37:26
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Invoice# 77-84993-84929.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Invoice# 77-84993-84929.exe'
Imagebase:	0xeb0000
File size:	1082880 bytes
MD5 hash:	3BEAA725263104D4638EB877A7D0B37D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.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	6DF0CF06	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	6DF0CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice# 77-84993-84929.exe.log	read attributes synchronize generic write	device	synchronous io non alert non directory file	success or wait	1	6E21C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Invoice# 77-84993-84929.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089", "C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6E21C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib.a152fe02a317a77aeec36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration.18d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core1fd8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xmlb219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile

Analysis Process: Invoice# 77-84993-84929.exe PID: 5732 Parent PID: 6104

General

Start time:	21:37:52
Start date:	13/01/2021
Path:	C:\Users\user\Desktop\Invoice# 77-84993-84929.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xf90000
File size:	1082880 bytes
MD5 hash:	3BEAA725263104D4638EB877A7D0B37D
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: 00000001.00000002.699728992.0000000006DE0000.00000004.00000001.sdmp, Author: Florian Roth - Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.699728992.0000000006DE0000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.699728992.0000000006DE0000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000001.00000002.699728992.0000000006DE0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.699774289.0000000006E20000.00000004.00000001.sdmp, Author: Florian Roth - Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.699774289.0000000006E20000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.699774289.0000000006E20000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000001.00000002.699774289.0000000006E20000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.699685453.0000000006DA0000.00000004.00000001.sdmp, Author: Florian Roth - Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.699685453.0000000006DA0000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.699685453.0000000006DA0000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000001.00000002.699685453.0000000006DA0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.699371662.0000000006C10000.00000004.00000001.sdmp, Author: Florian Roth - Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.699371662.0000000006C10000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.699371662.0000000006C10000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000001.00000002.699371662.0000000006C10000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.698742579.0000000005A61000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.698742579.0000000005A61000.00000004.00000001.sdmp, Author: Joe Security - Rule: NanoCore, Description: unknown, Source: 00000001.00000002.698742579.0000000005A61000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> - Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000001.00000002.699281215.0000000006B70000.00000004.00000001.sdmp, Author: Florian Roth - Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000001.00000002.699281215.0000000006B70000.00000004.00000001.sdmp, Author: Florian Roth - Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.699281215.0000000006B70000.00000004.00000001.sdmp, Author: Joe Security

[illegible]

	Rule: NanoCore, Description: unknown, Source: 00000001.00000002.695812658.0000000043B1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@technarchy.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	6DF0CF06	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	6DF0CF06	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	6CD5BEFF	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	6CD51E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Invoice# 77-84993-84929.exe:Zone.Identifier	success or wait	1	6CCD2935	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	unknown	8	b1 4f 3f 8e 4e b8 d8 48	.O?.N..H	success or wait	1	6CD51B4F	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DEE5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlibb1a152fe02a317a77ae36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEECA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbcb72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\18d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE403DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE403DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DEE5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD51B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD51B4F	ReadFile

Disassembly
