ID: 319577
Sample Name: eabass).exe
Cookbook: default.jbs
Time: 13:05:45
Date: 18/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

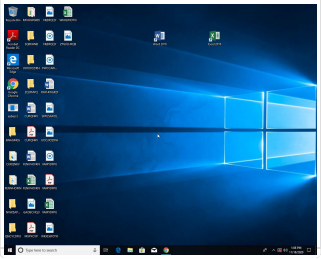
Analysis Report eabass).exe

Overview

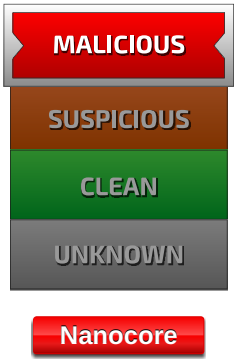
General Information

Sample Name:	eabass).exe
Analysis ID:	319577
MD5:	e104111a29db15..
SHA1:	b64fd544542b623.
SHA256:	563803e4673863..
Tags:	exe NanoCore RAT

Most interesting Screenshot:



Detection



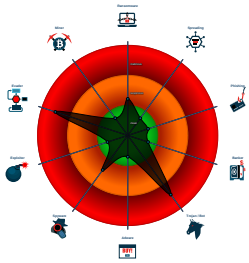
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Sigma detected: Scheduled temp file…
- Yara detected AntiVM_3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…

Classification



Startup

- **System is w10x64**
- eabass).exe (PID: 1144 cmdline: 'C:\Users\user\Desktop\eabass).exe' MD5: E104111A29DB150134FE6A812F54B691)
  - schtasks.exe (PID: 4624 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\iZjPEbxRTQJTJj' /XML 'C:\Users\user\AppData\Local\Temp\tmpEFB4.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5116 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - eabass).exe (PID: 2408 cmdline: C:\Users\user\Desktop\eabass).exe MD5: E104111A29DB150134FE6A812F54B691)
  - eabass).exe (PID: 4676 cmdline: C:\Users\user\Desktop\eabass).exe MD5: E104111A29DB150134FE6A812F54B691)
- **cleanup**

Malware Configuration

Threatname: NanoCore


```
{
  "C2: ": [
    "104.207.150.47"
  ],
  "Version: ": "NanoCore Client, Version=1.2.2.0"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.366661945.0000000003CB9000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xa7925:$x1: NanoCore.ClientPluginHost • 0xda145:$x1: NanoCore.ClientPluginHost • 0xa7962:$x2: IClientNetworkHost • 0xda182:$x2: IClientNetworkHost • 0xab495:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xddcb5:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
00000000.00000002.366661945.0000000003CB9000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.366661945.0000000003CB9000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xa768d:$a: NanoCore • 0xa769d:$a: NanoCore • 0xa78d1:$a: NanoCore • 0xa78e5:$a: NanoCore • 0xa7925:$a: NanoCore • 0xd9ead:$a: NanoCore • 0xd9ebd:$a: NanoCore • 0xda0f1:$a: NanoCore • 0xda105:$a: NanoCore • 0xda145:$a: NanoCore • 0xa76ec:$b: ClientPlugin • 0xa78ee:$b: ClientPlugin • 0xa792e:$b: ClientPlugin • 0xd9f0c:$b: ClientPlugin • 0xda10e:$b: ClientPlugin • 0xda14e:$b: ClientPlugin • 0xa7813:$c: ProjectData • 0xda033:$c: ProjectData • 0xa821a:$d: DESCrypto • 0xdaa3a:$d: DESCrypto • 0xafbe6:$e: KeepAlive
00000004.00000002.616576592.0000000003E8D000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.365898841.0000000002CB1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Click to see the 9 entries				

Unpacked PEs

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

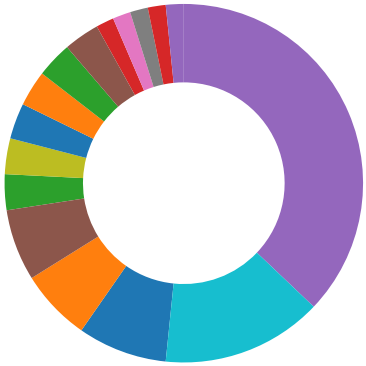
Sigma Overview

System Summary:

Sigma detected: NanoCore

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected 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:

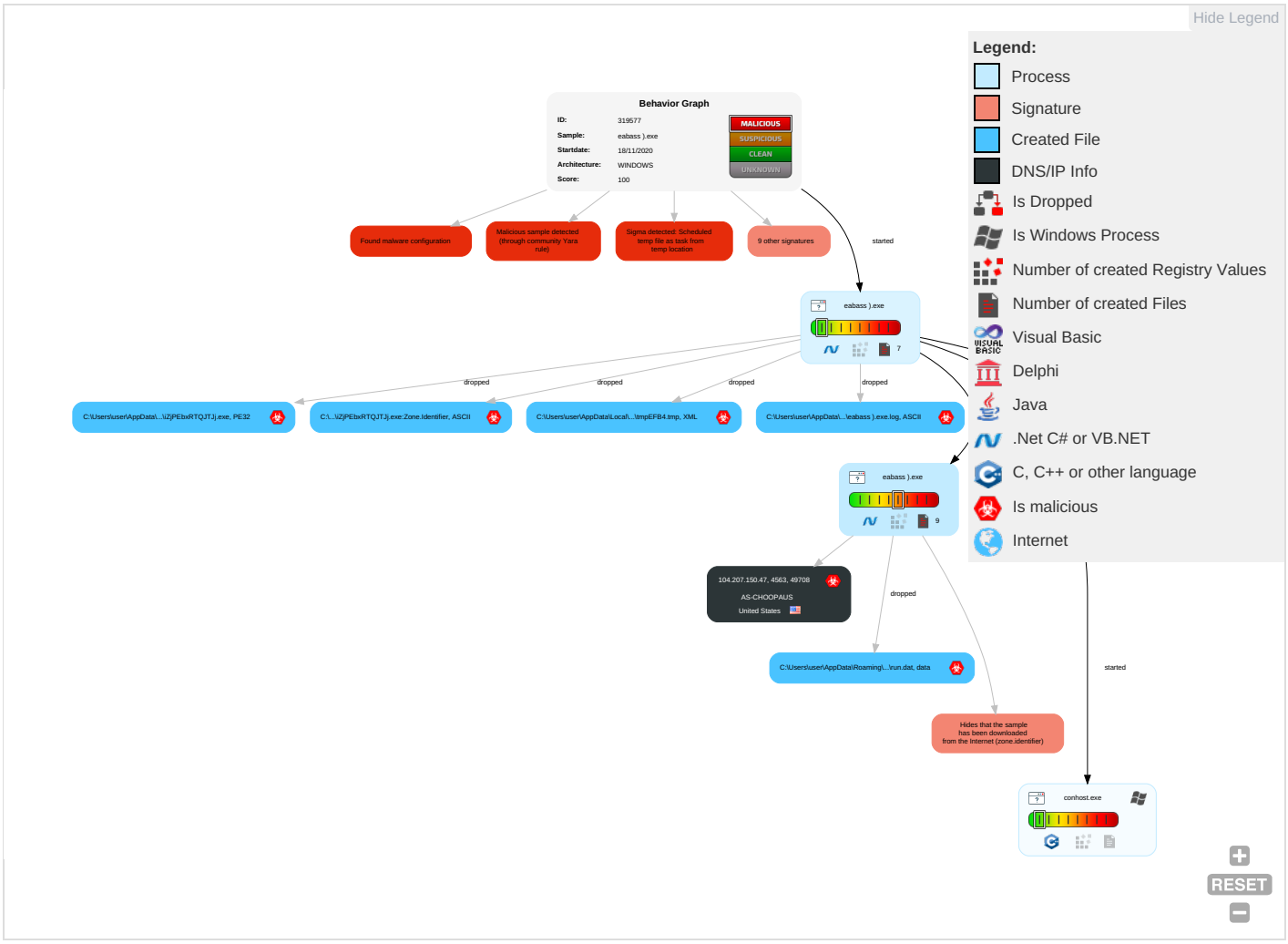
Detected Nanocore Rat

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	Ne Eff
Valid Accounts	Windows Management Instrumentation 1	Scheduled Task/Job 1	Process Injection 1 2	Masquerading 1	Input Capture 2 1	Security Software Discovery 1 2 1	Remote Services	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Ea Ins Ne Co
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Virtualization/Sandbox Evasion 3	LSASS Memory	Virtualization/Sandbox Evasion 3	Remote Desktop Protocol	Archive Collected Data 1 1	Exfiltration Over Bluetooth	Non-Standard Port 1	Ex Re Ca
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	Remote Access Software 1	Ex Tra Lo
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	SI Sw
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Ma De Co
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	System Information Discovery 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jar De Se
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Ro Ac
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Do Ins Pro

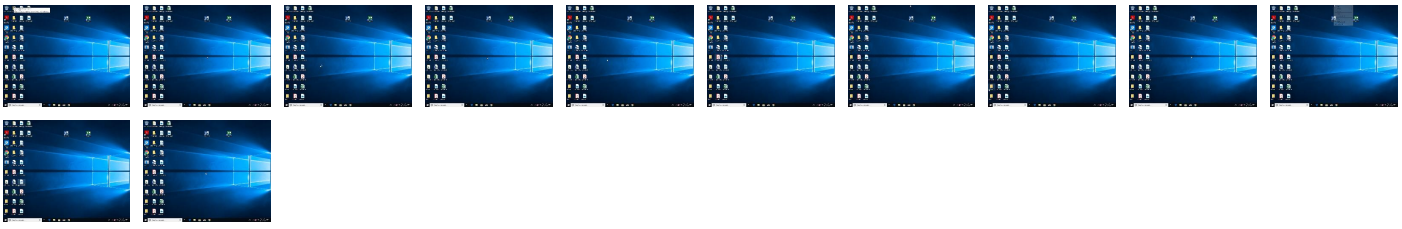
Behavior Graph



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
eabass).exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\iZjPEbxRTQJTJj.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.eabass).exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	eabass).exe, 00000000.0000000 2.365898841.0000000002CB1000.0 0000004.00000001.sdmp	false		high

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.207.150.47	unknown	United States		20473	AS-CHOOPAUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	319577
Start date:	18.11.2020
Start time:	13:05:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	eabass).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:	8
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@8/8@0/1
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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, WMIADAP.exe, svchost.exe • 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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:06:45	API Interceptor	1000x Sleep call for process: eabass).exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.207.150.47	Draft BL(s) (BL No UIH000062500).exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-CHOOPAUS	CpManyv2nV.exe	Get hash	malicious	Browse	• 108.61.29.35
	ubvk0T4ceG.exe	Get hash	malicious	Browse	• 108.61.29.35

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Hag4TPW3Ue.exe	Get hash	malicious	Browse	• 140.82.59.108
	2q8x6yYNHj.exe	Get hash	malicious	Browse	• 108.61.29.35
	oL9U4IbxMb.exe	Get hash	malicious	Browse	• 95.179.229.244
	Y7i2sl4Foh.exe	Get hash	malicious	Browse	• 140.82.59.108
	REibC3I4ju.exe	Get hash	malicious	Browse	• 108.61.29.35
	OBg8aUeQjJ.exe	Get hash	malicious	Browse	• 45.32.129.110
	tbzcpAZnBK.exe	Get hash	malicious	Browse	• 66.42.54.195
	w6r8DJTtvF.exe	Get hash	malicious	Browse	• 45.76.50.199
	fiksat.exe	Get hash	malicious	Browse	• 45.63.107.192
	Invoice.exe	Get hash	malicious	Browse	• 66.42.63.136
	qejrj9WOGM.exe	Get hash	malicious	Browse	• 140.82.59.108
	http://149.129.50.37/	Get hash	malicious	Browse	• 108.61.40.123
	RbM6WfSPbz.exe	Get hash	malicious	Browse	• 144.202.97.5
	PI210941.exe	Get hash	malicious	Browse	• 66.42.54.195
	document-359248421.xlsb	Get hash	malicious	Browse	• 45.63.107.192
	http://www.viportal.co	Get hash	malicious	Browse	• 209.250.225.52
	Amacon Order Specification Requirement.exe	Get hash	malicious	Browse	• 149.28.117.117
	4AXKXtaavC.exe	Get hash	malicious	Browse	• 140.82.59.108

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\eabass).exe.log

Process:	C:\Users\user\Desktop\eabass).exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1314
Entropy (8bit):	5.350128552078965
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEw:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHR
MD5:	1DC1A2DCC9EFAA84EABF4F6D6066565B
SHA1:	B7FCF805B6DD8DE815EA9BC089BD99F1E617F4E9
SHA-256:	28D63442C17BF19558655C88A635CB3C3FF1BAD1CCD9784090B9749A7E71FCEF
SHA-512:	95DD7E2AB0884A3EFD9E26033B337D1F97DDF9A8E9E9C4C32187DCD40622D8B1AC8CCDBA12A70A6B9075DF5E7F68DF2F8FBA4AB33DB4576BE9806B8E19180B7
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\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\f1d8480152e0da9a60ad49c6d16a3b6d\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=b77a

C:\Users\user\AppData\Local\Temp\tmpEFB4.tmp

Process:	C:\Users\user\Desktop\eabass).exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1659
Entropy (8bit):	5.176005492710507
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3Ctn:cbha7JlNQV/rydbz9I3YODOLNdq3u
MD5:	20AC5DF5C0E738DE92FB86366885E0CB
SHA1:	BF819154E2968870A6EF5E059DAE17B90A05993C
SHA-256:	01481B4B1EE586B5E2A93598F5F2ECAB905A8CA509776E0EAE5D1B95B1953988

C:\Users\user\AppData\Local\Temp\tmpEFB4.tmp	
SHA-512:	C4AB981CF70BE031AD18DE1D55B817A9114FD3AD5C771BD346CCFD63783504B9D7469F7B94662377E7B556098E1B1C6012F855E17F5C6CF514C203DD48B241F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
Process:	C:\Users\user\Desktop\eabass).exe
File Type:	data
Category:	dropped
Size (bytes):	232
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9
MD5:	32D0AAE13696FF7F8AF33B2D22451028
SHA1:	EF80C4E0DB2AE8EF288027C9D3518E6950B583A4
SHA-256:	5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29
SHA-512:	1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C356A5
Malicious:	false
Reputation:	moderate, very likely benign file
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.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\eabass).exe
File Type:	data
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:u09t:uE
MD5:	F85BF482C98AF76102C8E65250639E50
SHA1:	F46E7F19C2F16FDD3EAB9D60F4064B5BBEE8D952
SHA-256:	BDE0B0543A8C7AACA18EBB5A7A2694344BBE3BFD5D2127037E7AD183B815F88B
SHA-512:	5CA469F597C2EB393D83D1B8AB7FD073E47558D8EFA251DB9D6BB6389E35E6C79B32796AF1A9592E4447F2EDC668229450E0A9C644E8D9BB157B305091599848
Malicious:	**true**
Reputation:	low
Preview:	t.O....H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\eabass).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:	1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671ECB
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\eabass).exe
File Type:	data

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Category:	dropped
Size (bytes):	327432
Entropy (8bit):	**7.99938831605763**
Encrypted:	**true**
SSDEEP:	6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm
MD5:	7E8F4A764B981D5B82D1CC49D341E9C6
SHA1:	D9F0685A028FB219E1A6286AEFB7D6FCFC778B85
SHA-256:	0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480
SHA-512:	880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^.....>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i.....J.5b7}..fK..HV.,...0.... ....n.w6PMl.....v.'".v.....#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.QI..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.....Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.\|i4...i...;O...n.?.,. ....v?.5}.OY@.dG\|<.._[.69@.2..m..I..oP=...xrK.?.....b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.....H...6$. ..d...|m...N..1.R..B.i.....$....$.....CY}..$....r....H...8...li.....7 P.....?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7

C:\Users\user\AppData\Roaming\iZjPEbxRTQJTJj.exe	
Process:	C:\Users\user\Desktop\eabass).exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	665088
Entropy (8bit):	7.696568668619478
Encrypted:	false
SSDEEP:	12288:H6jXmxXRv6+ftJuI2TBFbsZni3lcEs2jMJ7KUZt9luz9NK3vSH:ZBvvftJuI21aZWGEsrJ7KU5M23qH
MD5:	E104111A29DB150134FE6A812F54B691
SHA1:	B64FD544542B623F37778EDE23AE39CA508ED868
SHA-256:	563803E4673863857F98356D9D8177B4D1AFB49E8EB839E80E4F6E416E7F1083
SHA-512:	12C9223B2D3FC712883CB97FDADF03CDB1EC775B8BE102C0537153C54AF4CDEB4D46DC4AAF2333627984321A424B3ABAA6A00E1E61D5480226680322BE2BA2A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....._.....P.....^:... ...@....@.. ....@.....:...S....@.....`..... ..... ..H.....text...d.... ..... ..`.rsrc.....@.....@..@..rel oc.....`.....$.....@..B.....@:.....H.....0.....`.....*....(!.....("....(#.....($.....(%....*N..(....o....(&....*&..('....*.s(.....s).....s*.....s+.. .....s,.....*Z.....o?.....*&..(@....*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{....(...+}.....{....+.*j..{.

C:\Users\user\AppData\Roaming\iZjPEbxRTQJTJj.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\eabass).exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.696568668619478

General

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	eabass).exe
File size:	665088
MD5:	e104111a29db150134fe6a812f54b691
SHA1:	b64fd544542b623f37778ede23ae39ca508ed868
SHA256:	563803e4673863857f98356d9d8177b4d1afb49e8eb839 80e4f6e416e7f1083
SHA512:	12c9223b2d3fc712883cb97fdadf03cdb1ec775b8be102c 0537153c54af4cdeb4d46dc4aaf2333627984321a424b3a baa6a00e1e61d5480226680322be2ba2da
SSDEEP:	12288:H6jXmxXRv6+ftJuI2TBFbsZni3lcEs2jMJ7KUZt9l uz9NK3vSH:ZBvvftJuI21aZWGEsrJ7KU5M23qH
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L..... ._.....P.....^`... ...@....@.. ....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a3a5e
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:	0x5FB4FACB [Wed Nov 18 10:43:23 2020 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
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
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	0xa3a08	0x53	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xa4000	0x5b0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xa6000	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	0xa1a64	0xa1c00	False	0.81880162046	data	7.7057574273	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xa4000	0x5b0	0x600	False	0.423828125	data	4.09731810024	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xa6000	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	0xa40a0	0x324	data		
RT_MANIFEST	0xa43c4	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 2017 - 2020
Assembly Version	1.0.0.0
InternalName	WMLJ.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	CashMe Out
ProductVersion	1.0.0.0
FileDescription	CashMe Out
OriginalFilename	WMLJ.exe

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:06:57.161761999 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:57.342571974 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:57.342952967 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:57.434830904 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:57.620856047 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:57.621068954 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:57.854350090 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:57.855804920 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.035903931 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.065124989 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.290086985 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.290112019 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.290128946 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.290144920 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.292371988 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.472335100 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.472367048 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.472383022 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.472395897 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.472409010 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.472429037 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.472445965 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.472461939 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.472552061 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.472585917 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.652507067 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.652535915 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.652559042 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.652581930 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.652597904 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.652597904 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.652614117 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.652631044 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.652636051 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.652653933 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.652672052 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.652712107 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.653127909 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.653147936 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.653168917 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.653187037 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.653189898 CET	49708	4563	192.168.2.6	104.207.150.47

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 18, 2020 13:06:58.653203964 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.653223038 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.653232098 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.653245926 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.653283119 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.653335094 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.654036999 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.832644939 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832674026 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832689047 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832701921 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832717896 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832736969 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832755089 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832772970 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832784891 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832801104 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832803011 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.832819939 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832838058 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832854986 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832863092 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.832870960 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832886934 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832901001 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.832901955 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.832925081 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.832966089 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.832983971 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833000898 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833059072 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.833070993 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833089113 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833105087 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833121061 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833137989 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833157063 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833172083 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.833173990 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833189964 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833204985 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833220959 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833223104 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.833236933 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833251953 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.833259106 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.833316088 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:58.834074020 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.834094048 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:58.834188938 CET	49708	4563	192.168.2.6	104.207.150.47
Nov 18, 2020 13:06:59.013355017 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:59.013382912 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:59.013400078 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:59.013416052 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:59.013433933 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:59.013453007 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:59.013472080 CET	4563	49708	104.207.150.47	192.168.2.6
Nov 18, 2020 13:06:59.013488054 CET	4563	49708	104.207.150.47	192.168.2.6

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: eabass).exe PID: 1144 Parent PID: 5952

General

Start time:	13:06:44
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\eabass).exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\eabass).exe'
Imagebase:	0x870000
File size:	665088 bytes
MD5 hash:	E104111A29DB150134FE6A812F54B691
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: 00000000.00000002.366661945.0000000003CB9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.366661945.0000000003CB9000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.366661945.0000000003CB9000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.365898841.0000000002CB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.365991657.0000000002D09000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

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	6DEBCF06	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	6DEBCF06	unknown
C:\Users\user\AppData\Roaming\iZjPEbxRTQJTJj.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CD0DD66	CopyFileW
C:\Users\user\AppData\Roaming\iZjPEbxRTQJTJj.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CD0DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmpEFB4.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CD07038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\eabass).exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E1CC78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEFB4.tmp	success or wait	1	6CD06A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\iZjPEbxRTQJTJj.exe	0	262144	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 cb fa b4 5f 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 1c 0a 00 00 08 00 00 00 00 00 00 5e 3a 0a 00 00 20 00 00 00 40 0a 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0a 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L......_.......... ....P............^:... ...@....@.. ....@.................	success or wait	3	6CD0DD66	CopyFileW
C:\Users\user\AppData\Roaming\iZjPEbxRTQJTJj.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CD0DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEFB4.tmp	unknown	1659	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 65 6e 67 69 6e 65 65 72 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </Registratio	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\eabass).exe.log	unknown	1314	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E1CC907	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile

Analysis Process: schtasks.exe PID: 4624 Parent PID: 1144

General

Start time:	13:06:52
Start date:	18/11/2020
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\iZjPEbxRTQJTJj' /XML 'C: \Users\user\AppData\Local\Temp\tmpEFB4.tmp'
Imagebase:	0xaf0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpEFB4.tmp	unknown	2	success or wait	1	AFAB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmpEFB4.tmp	unknown	1660	success or wait	1	AFABD9	ReadFile

Analysis Process: conhost.exe PID: 5116 Parent PID: 4624

General

Start time:	13:06:52
Start date:	18/11/2020
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: eabass).exe PID: 2408 Parent PID: 1144

General

Start time:	13:06:52
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\eabass).exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\eabass).exe
Imagebase:	0x1c0000
File size:	665088 bytes
MD5 hash:	E104111A29DB150134FE6A812F54B691
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: eabass).exe PID: 4676 Parent PID: 1144

General

Start time:	13:06:53
Start date:	18/11/2020
Path:	C:\Users\user\Desktop\eabass).exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\eabass).exe
Imagebase:	0x9a0000
File size:	665088 bytes
MD5 hash:	E104111A29DB150134FE6A812F54B691
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.616576592.0000000003E8D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000004.00000002.612290722.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000004.00000002.612290722.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.612290722.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: NanoCore, Description: unknown, Source: 00000004.00000002.613779714.0000000002E48000.00000004.00000001.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	6DEBCF06	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	6DEBCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CD0BEFF	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	6CD01E60	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	6CD0BEFF	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	6CD0BEFF	CreateDirectoryW
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	6CD01E60	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	6CD01E60	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	6CD01E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\eabass).exe:Zone.Identifier	success or wait	1	53E7C7E	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	74 ed 4f e1 05 8c d8 48	t.O....H	success or wait	1	6CD01B4F	WriteFile
C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	unknown	232	47 6a 93 68 5c a3 33 c7 ba 41 97 d8 c4 35 b2 78 95 96 26 15 ab 98 69 2b 98 cd 89 63 28 31 a3 50 c6 e5 50 83 63 4c 54 a1 9f c5 82 41 c5 62 c9 e2 1b 95 b8 f0 f0 e7 34 68 a6 12 b5 74 bc 2b f0 07 5a 5c b0 bf 20 9f 69 cc 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 93 0b a6 73 7e 82 c7 46 04 b7 fb 7d 99 ad 83 81 ed 81 00 45 f9 c7 db f0 db f0 45 f9 14 f3 b4 36 45 8f 94 b5 81 a3 7b d9 9f 05 18 7b ed a9 79 53 82 bd bf 37 fa c4 22 16 68 4b d7 21 03 78 86 32 be 99 69 df a3 8f 7a 4a d5 da bb fa 20 fc b4 c0 c0 66 d0 dd a7 3f c0 5f 0b e4 fb a3 30 ca 3a 65 5b 37 77 7b 31 81 21 de 34 a9 bb 99 d3 ca 26 b9	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.. ...s~..F...}.....E.....E... .6E.....{....{..yS...7..".hK.! .x.2..i...zJ.... ....f...?._.. ..0.:e[7w{1.!.4.....&.	success or wait	1	6CD01B4F	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	327432	70 54 c7 ab ad 21 b0 08 57 f6 fa 47 14 4a ba aa 61 dd a0 29 17 40 c6 8b 69 8b df 77 70 4b 98 73 6f 40 e2 06 e5 35 e7 b7 3d e9 b8 90 5e ab 1d 51 82 6f 79 f9 3d 65 40 39 c3 42 8d f7 95 46 bc cb 30 39 75 22 33 8b f5 20 30 74 c0 19 52 44 6e 5f 34 64 fb b8 17 02 df 45 c0 90 06 69 f4 08 9f ae bb 8a 7e 0c 89 85 7c 87 eb 66 58 5f 0e c2 ed 58 66 88 70 5e e2 f5 ff 94 03 e5 3e 61 db 8b 91 24 8d 8a 8f 65 05 36 3a 37 64 b6 28 61 05 41 e4 fe e0 3d be 29 2a 0d 96 a8 90 8e 7b 42 1c 5b ab 87 cb 79 25 b3 2a e4 b8 b1 9f 69 a7 51 84 3c f3 94 a2 90 78 74 c4 a9 58 13 11 48 09 d7 20 ad cc a4 48 46 37 67 0f e0 c5 49 96 2a 33 03 7b 0c 6e 92 bf 90 be 4c d1 9b 79 3b 69 87 bc 73 2d 1e b6 f9 b8 28 35 69 c2 8b 92 d6 10 ac a7 02 93 ee 89 08 17 4a 09 35 62 37 7d fe 86 66 4b af ab 48 56	pT...!..W..G.J..a..).@..i..wpK .so@...5..=...^..Q.oy.=e@9 .B...F..09u"3.. 0t..RDn_4d.....E.. .i.....~...|..fX_....Xf.p^.... ..>a...$...e.6:7d.(a.A...=.)*. ....{B.[...y%.*....i.Q.<....xt ..X..H.. ...HF7g...I.*3.{.n... .L..y;i..s-....(5i..... .J.5b7}..fK..HV	success or wait	1	6CD01B4F	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	6CD01B4F	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	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DE95705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE9CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DDF03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DDF03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6DE95705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CD01B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CD01B4F	ReadFile
C:\Users\user\Desktop\eabass).exe	unknown	4096	success or wait	1	6DE7D72F	unknown
C:\Users\user\Desktop\eabass).exe	unknown	512	success or wait	1	6DE7D72F	unknown

Disassembly

Code Analysis