ID: 625008
Sample Name: aSsc9zh1ex
Cookbook: default.jbs
Time: 10:30:45
Date: 12/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Disassembly 21

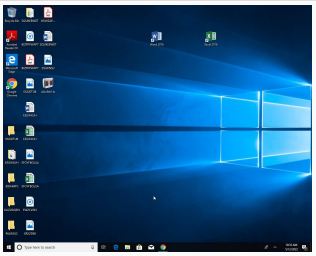
Windows Analysis Report

aSsc9zh1ex

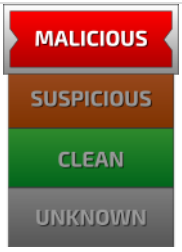
Overview

General Information

Sample Name:	aSsc9zh1ex (renamed file extension from none to exe)
Analysis ID:	625008
MD5:	d5e55a57372bca..
SHA1:	9b1935a927c072..
SHA256:	3c27c2aa1bc826..
Tags:	32 exe trojan
Infos:	



Detection



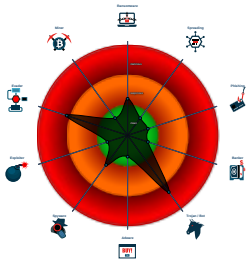
GuLoader

Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Tries to detect virtualization through…
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- Sample file is different than original …
- PE file contains strange resources
- Drops PE files
- Contains functionality to shutdown /…
- Uses code obfuscation techniques (…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- aSsc9zh1ex.exe (PID: 4152 cmdline: "C:\Users\user\Desktop\aSsc9zh1ex.exe" MD5: D5E55A57372BCAD45FBB260105179CAF)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "http://barsam.com.au/bin_QuCucbUMda229.bin"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.886415142.0000000002D70000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

Data Obfuscation

Yara detected GuLoader

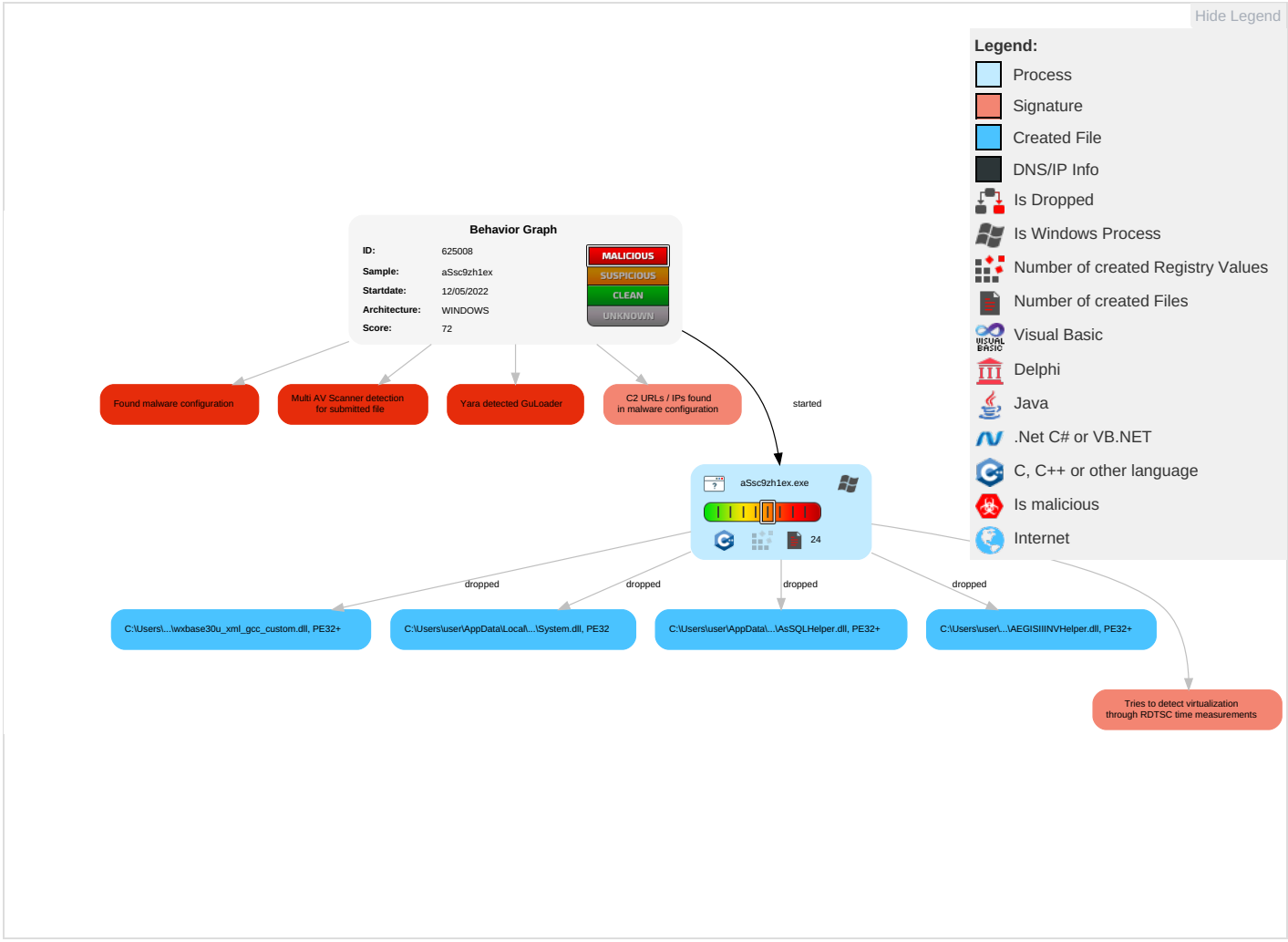
Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	Path Interception	1 Access Token Manipulation	1 Access Token Manipulation	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Obfuscated Files or Information	LSASS Memory	2 File and Directory Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 3 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data

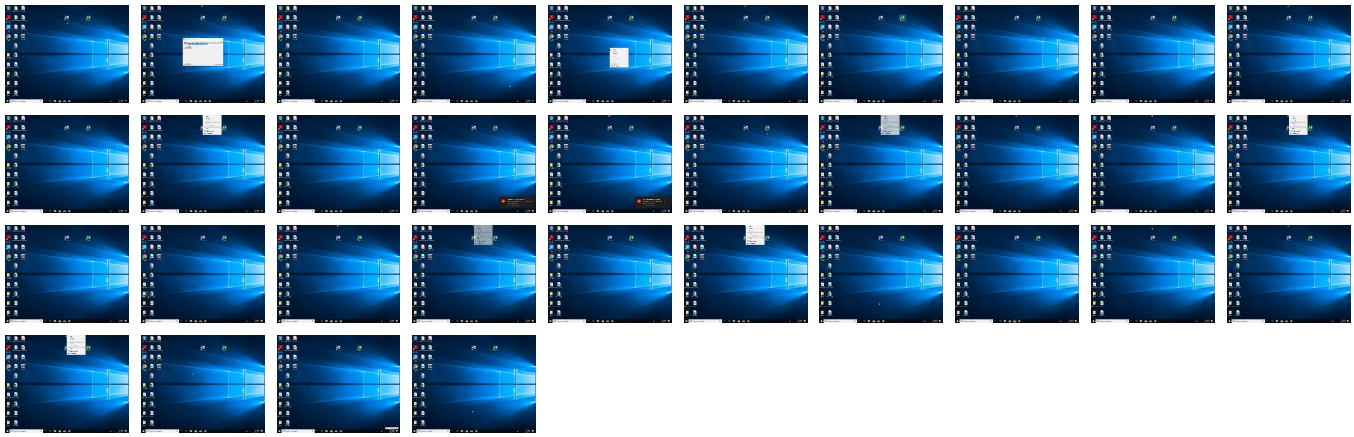
Behavior Graph



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
aSsc9zh1ex.exe	38%	Virustotal		Browse
aSsc9zh1ex.exe	14%	Metadefender		Browse
aSsc9zh1ex.exe	34%	ReversingLabs	Win32.Downloader.GuLoader	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://barsam.com.au/bin_QuCucbUMda229.bin	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0C	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://barsam.com.au/bin_QuCucbUMda229.bin	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	aSsc9zh1ex.exe, 00000001.00000002.886112266.0000000000788000.00000004.00000001.01000000.00000005.sdmp, wxbase30u_xml_gcc_custom.dll.1.dr	false	• URL Reputation: safe	unknown
http://nsis.sf.net/NSIS_ErrorError	aSsc9zh1ex.exe	false		high
http://ocsp.sectigo.com0	aSsc9zh1ex.exe, 00000001.00000002.886112266.0000000000788000.00000004.00000001.01000000.00000005.sdmp, wxbase30u_xml_gcc_custom.dll.1.dr	false	• URL Reputation: safe	unknown
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	aSsc9zh1ex.exe, 00000001.00000002.886112266.0000000000788000.00000004.00000001.01000000.00000005.sdmp, wxbase30u_xml_gcc_custom.dll.1.dr	false	• URL Reputation: safe	unknown
http://https://sectigo.com/CPS0C	aSsc9zh1ex.exe, 00000001.00000002.886112266.0000000000788000.00000004.00000001.01000000.00000005.sdmp, wxbase30u_xml_gcc_custom.dll.1.dr	false	• URL Reputation: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	625008
Start date and time: 12/05/202210:30:45	2022-05-12 10:30:45 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	aSsc9zh1ex (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:	17

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:	mal72.troj.evad.winEXE@1/8@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 85.5% (good quality ratio 84.2%) • Quality average: 87% • Quality standard deviation: 21.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.125.122.176
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com, login.live.com, sls.update.microsoft.com, ctldl.windowsupdate.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com, glb.sls.prod.dcat.dsp.trafficmanager.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	60648
Entropy (8bit):	6.273540391388373
Encrypted:	false
SSDEEP:	768:VyIscWONgNnXigWuv3uuCRCF5AElVllzCix92FBo/SlOKsVjiVsRb2X9bhM:VDt5Ngg23TgNElDNeo/8OLjiOR6
MD5:	00B917A158BB5BF0D6BFF7D6B3C81B12
SHA1:	24A9B80C8EC794ADA4C8BAF717CFAB98459AC1DE
SHA-256:	947BE059906893C09F222CB2868631638A219FB905A47E16A311BA5ADEB4B300
SHA-512:	47B8EABDF404E19B2D953933D2D0C922CC538B3876D7664110CBD739605FFD151D24788E60B9935E6E4F7BB463F6BC7CED253CF31ED5C4D210495C301C7E5F5
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@..... .....!..L.!This program cannot be run in DOS mode....$.....P..K1.K1.K1.BIX.G1..Y.I1....J1..Y.D1..Y.C1..Y.H1.BIO.J1.BIH.J 1.8S.N1.K1..1..X.H1..X.J1..X4.J1.K1\.J1..X.J1.RichK1.....PE..d....5;a....." .....j.....0..... ....`.....`..... .....H..... ..4.....p..... .....text..... ..`.rdata.. -.....@..@.data...`.....@....pdata. .....@..@.rsrc...H.....@..@.reloc..4.... .....@..B..... .....

C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	36576
Entropy (8bit):	6.18658407883376
Encrypted:	false
SSDEEP:	384:Vw33667/fhcAcwuVQydIDddeypaROhGkXMV3lBhjUK98krmRt8ZrqL1r8/lSNriq:q33oWsUK98vAqL1r8oFiQ7b2X9shHf
MD5:	0B849C073801DCE25301ECA0146D534B
SHA1:	5BB9251CA83FE96C8F52B35637E674A629ED1468
SHA-256:	3F77E9EF8843DE3DA37037F21BCF6D7E990085D2BDC5B3F05E71AB5EBE5288BB
SHA-512:	1C5C99BD93FBACD3BA56ADE806092AB86BA3FEA0BB70DE0FB89775285A71DB47F2400CF29757370CDC69F13FCBCF6513B25F4C8BBED0A15D65A9618BEE733A7F
Malicious:	false
Antivirus:	• Antivirus: Virustotal, Detection: 0%, Browse • Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$....._.%.>.v.>.v.>.v.FNv.>.v.\.w.>.v.V.w.>.v.V.w.>.v.V.w.>.v.V.w.> .v.`.w.>.v.>.v.>.v!W.w.>.v!W.w.>.v!W"v.>.v.>Jv.>.v!W.w.>.vRich.>.v.....PE..d.....a....." ....>..\.....@..... ..... .....pd..l....d.....p.....H....T..p.....`U.....P.....text....<.....>..... ..`.rdata.....P.....B.....@..@.data...0....p.....`.... .....@....pdata.....b.....@..@.rsrc.....h.....@..@.reloc..H.....n.....@..B..... .....

C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1070
Entropy (8bit):	4.836891219007383
Encrypted:	false
SSDEEP:	24:JdtGOiNK+bIg4y3QdM/Ai8qTCNzgDQRnKVGaQkl:3U1K+bIg4y3QdaIzgDQh3aQkl
MD5:	9B48061E7B9FC35CD2624F2B9102549E
SHA1:	9DA640A8AF809549031916AB143026FAAF3B1E74
SHA-256:	84839C6E85F9B73AA6B0F331A9EAADF7409B7B36E30BA0B04E31680069103E43
SHA-512:	01CF7B5CBDEB1038E79076CB452AC63B0037C86570C3FE97B6C559823F43D515F34CAC963D3737B9EAF103F0EBDEBC1317B68091D4332C3615E87A3F25DF679E
Malicious:	false

Reputation:	low
Preview:	.<?xml version="1.0" encoding="UTF-8" standalone="yes" ?>..<assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0">.. <dependency>.. <dependentAssembly>.. <assemblyIdentity type="win32" name="Microsoft.Windows.Common-Controls" version="6.0.0.0" processorArchitecture="x86" publicKeyToken="6595b64144ccf1df" language="*" />.. </dependentAssembly>.. </dependency>.. <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">.. <security>.. <requestedPrivileges>.. <requestedExecutionLevel level="asInvoker" uiAccess="false" />.. </requestedPrivileges>.. </security>.. </trustInfo>.. <dependency>.. <dependentAssembly>.. <assemblyIdentity name="NeGACOM" type="win32" version="17.0.0.0" processorArchitecture="x86" />.. </dependentAssembly>.. </dependency>.. <dependency>.. <dependentAssembly>.. <assemblyIdentity name="OnlineServices" version="17.0.0

C:\Users\user\AppData\Local\Temp\Strepera.wad

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	data
Category:	dropped
Size (bytes):	77432
Entropy (8bit):	6.5191464617024995
Encrypted:	false
SSDEEP:	1536:0ryhqjc8wTqJ39FNvl4UXgmBfCotcEntclFVdwJZp:0ryTk3HdyYgmBfCscEilFVG
MD5:	0CAED7F18389A6CC24391E0400C2BE47
SHA1:	59288CED440D46970090F25983B409BB25F43BBF
SHA-256:	E8C48296D444C8EDBF6169CA9E3C5334B0813BFC684C2E99BFD61C692A3784F1
SHA-512:	AFC59C8EA01D5F96DFAB3CD08F088FF2136542C0F13435EE9D63795CD8BDEF6D7464082968 83CD9052BF21D6E87388295B4682F06913CC982B21868704277B93
Malicious:	false
Reputation:	low
Preview:	....f.f.....GE.......z.I.J=.yk.....W[...o....6......O-P.j"q..h.r...m.v..X...F.1.BV..p.,....Td...L|c.A.._C.....~.7ws...4.Z...$...>..e.YS...&..I..._.....}.a;'a..g*Y.DN.Ql.`.(+#;.....%3...]..u..\K.8..<f./.)..w.0.I..:n.x..Nt{.....?^..M580H. C...d2@..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.j"q..h.r...m.v..X...F.1.BV..p.,....Td...L\|c.A.._C.....~.7ws...4.Z...$..>..e.YS...&.....}.a;'a..g*Y.DN.Ql.`.(+#;.....1.....k..|3...]..u..\K.8..<f./.)..w.0.I..:n.x..Nt{.....?^..M580H. C...d2@..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.....n....."q..h.r...m.v..X...F.1.BV..p.,....Td...L|c.A.._C.....~.7ws...4.Z...$...>..e.YS...&.....}.a;'a..g*Y.DN.Ql.`.(+#;.....%3...4.*..:.....]..u..\K.8..<f./.)..w.0.I..:n.x..Nt{.....?^..M580H. C...d2@..!..U..R%i.GE.....z.I.J=.yk.....W[...o....6.....O-P.j"q..h.r...m.v..X...F.1.BV.....f.....p.,....Td...L\|c.A.._C.....~.7ws...4.Z...$...>..e.YS.

C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	288
Entropy (8bit):	7.002703251110111
Encrypted:	false
SSDEEP:	6:6v/lhPysDjYOGW78zHS1w9xuIGXdvkFRBp9rXHEb/GY1IX2NYKjp:6v/7jjYOGW7Rw9xu6pxHG/VIX6F
MD5:	A83F8C904AFA9E3F6A50D263747CF6DF
SHA1:	7B9D99B950518FCAF5AC59350823D2B20E82956F
SHA-256:	F57C0B31EC836E26EB609F259CFA68DDA95F09685784423B61075DAE4BBA5BF6
SHA-512:	4B2DC243E86514BDC816B92808C491EF71B72690F25C2372FE909CED3A103F990708C507065169FA5C6F823A8B1ADADB7BF13696E78C807A973789CF14CA3A0
Malicious:	false
Reputation:	low
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....IDAT8...N.Q...'.....X.s.^../H.f.....BJ....V[.b..qsvA..d..y.9?...z.`./....'..[.Q..'...M.....mwuN.\....h..(|.....p.K..I.%..... ..*..x.t~.kW.`V'.8.W.K.I.4..9.&\..k..3F.....4.0.op.rL#.....N:.=.T.[....L.....p...#....IEND.B`.

C:\Users\user\AppData\Local\Temp\face-crying.png

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	893
Entropy (8bit):	7.712327619290152
Encrypted:	false
SSDEEP:	12:6v/7M/6CsI5hmePcdiB6BV3h8SkKc47zOTtcC8VErf6qdY94OR/vlNMgmaGe7fb:q65hBcs6L3h6hBcCLrDq42nMDanb
MD5:	473EE416AF2C1AE05AA7D5D004C9B3D2
SHA1:	EEC352E25F562C0386D5C92384A70B3005D40D6F
SHA-256:	2C48F1719BBC825592FB0929E31DCFE66578665D28099087EA98EF261688DC18
SHA-512:	2B05C9920CFDCF378448F35B14AA56078051584CA0DB15F43B5A27272B072DD8A76BBC2829DF4C7C7BAF8339839974A00CA7BFFB8425B7D9494421CCC9EE80 1
Malicious:	false

Preview:	.PNG.....IHDR.....a...DIDATx.e.C..H.F_..tzl{m.m.m.m..;=F+..j.....r.....hZ...%Sn...Z....|g...o.c..f..k..#.Y.5..2...r44.t...[|.EW....E..3v....o...n...y.V.%.\g.].XY.).PQ..h~ .Mu.!.~.!{dt...-....c.....~.ihs..<.23h.q...AA....P.O.d.#....S%....w....~(.Yg.mL.`..r.U?A.D.....%.t..~.b..wl...G\r.....,^m.b%..??...?./.....O..w|..t..5...^x....cK..?..b...3^#i.xYp3 .>..C<Q.yg^.3.=..;./..!.`.....dq%...`..wB....q.2....W....S`....E....q3.A....9...."..].+.f...-.Z)d*..h..O>.....c>...=.P..!...pw}g..t&.=..Dd...i.f.....\....-JO0hW....!.ic.%...s.+...iG|..MK.. .O_..;_.q_....|...F....M...O...o..5.=...y{...]hn..Z..L+..`r.&I...5t._Dz..m.~$n$..|.u}_.n|.53..b.+Zn.bCA.1..x..hv?.{8...!\J.....>OukN..{...[#.....7....k..L.#...D.y:K5.|.&..XV.U..rb..T..G..6. I...~.....i.#ike...9/B_&.....^v]..._.I.Et.i..M..I.B1...A.....>._...P.,... ....IEND.B`.

C:\Users\user\AppData\Local\Temp\nsc4B5D.tmp\System.dll

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... ....."..... ..`.rdata..c....@.....&.....@..@.data...x....P.....*.....@....reloc.....`.....,.....@..B..... ....

C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll

Process:	C:\Users\user\Desktop\aSsc9zh1ex.exe
File Type:	PE32+ executable (DLL) (console) x86-64 (stripped to external PDB), for MS Windows
Category:	dropped
Size (bytes):	214568
Entropy (8bit):	6.30310219025288
Encrypted:	false
SSDEEP:	3072:WSQvJRT4XDaGZcJRQqnKJNuC3d5C/I4ye9P7Vvw/YDQzix+AKp:WDRT4XDpZ0QqnKJNuCwx9PRCixK
MD5:	6D01A897D44DD4D25D7E1264407210FD
SHA1:	332C3ADE84D0C1E5BE298C037F9FE222620343B2
SHA-256:	DD8289A21902F458B861C08A2F54D23F1E214B37BB89E73D4108303B490F7644
SHA-512:	54098533FDC9B4BAB0CD525D652846B5CDCD808089346D0192D7CF9DE6C1E8E329E2071886391D729F3DFED59D2E860E8A811E07E6688E6AA0B55D5D98D1AD D
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....".#.B.....P.....d.....2... ..`... .....P.....`.....".(S.....@...(.....c..8.....text....A.....B.....`.P`.data.....`.....F.....@. `..rdata..\....p.....H.....@.`@.pdata.....@.0@.xdata..... .....@.0@.bss.....@.....`..edata.....P.....@.0@.idata.. .....`.....@.0..CRT....X.....@.@..tls.....@.@..rsrc.....@.0..reloc.....@.0B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.537994904334399
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	aSsc9zh1ex.exe
File size:	326847
MD5:	d5e55a57372bcad45fbb260105179caf
SHA1:	9b1935a927c072dd31017362ff1739bf1ea2aaf7
SHA256:	3c27c2aa1bc826faa65ab4038eb385cabd6db50108410e6f674d455aa1dc5532
SHA512:	088033564668a4fd3e107566387fecf0b6dcbd7a161c9ef3e4adb232520467a64af9eec740fe783d5c62fa3b79bdd910e72f3acc838e5fa155427c83003c407b
SSDEEP:	6144:13yztyL/0/bbdat6J9mOnuuAgo+/sOxCHBs4YIwUrJrnBpKussJ9LQu:13pL0/bbdat6JIO1Ag2TBs4YI3BnB35N
TLSH:	07640144E6684D21FCBA0D3C0533D4A76974CC220879DBBB2BAE751A2BF51D1822FD67

File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....!`G.@...@...@../OQ..@...@..I@../OS..@...c>..@..+F...@..Rich.@.....PE..L...h.Oa.....h....:....

File Icon

Icon Hash:	c8fbb7a7a7e3f80c

Static PE Info

General

Entrypoint:	0x40350a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9A68 [Sat Sep 25 21:53:44 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	56a78d55f3f7af51443e58e0ce2fb5f6

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A2E0h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080CCh]
mov esi, dword ptr [004080D0h]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FED0073078Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi

Instruction
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FED0073075Ah
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [007A8B18h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x3d6000	0x15908	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
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	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6670	0x6800	False	0.667931189904	data	6.43600264122	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.45	data	5.14577456407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x39eb78	0x600	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.ndata	0x3a9000	0x2d000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3d6000	0x15908	0x15a00	False	0.471132135116	data	5.8124427271	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x3d62c8	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x3e6af0	0x25a8	data	English	United States
RT_ICON	0x3e9098	0x10a8	data	English	United States
RT_ICON	0x3ea140	0x988	data	English	United States
RT_ICON	0x3eaac8	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x3eaf30	0x100	data	English	United States
RT_DIALOG	0x3eb030	0x11c	data	English	United States
RT_DIALOG	0x3eb150	0xc4	data	English	United States
RT_DIALOG	0x3eb218	0x60	data	English	United States
RT_GROUP_ICON	0x3eb278	0x4c	data	English	United States
RT_VERSION	0x3eb2c8	0x300	data	English	United States
RT_MANIFEST	0x3eb5c8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, CreateFileW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Avnet, Inc.
FileVersion	24.30.26
CompanyName	Stewart Information Services Corp
LegalTrademarks	PacifiCare Health Systems Inc
Comments	Reliance Steel & Aluminum Co.
ProductName	Mariner Health Care Inc.
FileDescription	Disc Soft Ltd
Translation	0x0409 0x04b0

Possible Origin		
Language of compilation system	**Country where language is spoken**	**Map**
English	United States	

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: aSsc9zh1ex.exe PID: **4152**, Parent PID: **1964**

General	
Target ID:	1
Start time:	10:31:53
Start date:	12/05/2022
Path:	C:\Users\user\Desktop\aSsc9zh1ex.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\aSsc9zh1ex.exe"
Imagebase:	0x400000
File size:	326847 bytes
MD5 hash:	D5E55A57372BCAD45FBB260105179CAF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000001.00000002.886415142.0000000002D70000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsw48CC.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406078	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\nsc4B5D.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	406078	GetTempFileNameW

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsc4B5D.tmp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	405A94	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\nsc4B5D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\nsc4B5D.tmp\System.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	object name collision	17	406036	CreateFileW
C:\Users	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	405AD4	CreateDirectoryW
C:\Users\user\AppData\Local\Temp\Strepera.wad	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	406036	CreateFileW

<table>
<tr><th>File Path</th><th>Access</th><th>Attributes</th><th>Options</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>406036</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>406036</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\face-crying.png</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>406036</td><td>CreateFileW</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll</td><td>read attributes | synchronize | generic write</td><td>device</td><td>synchronous io non alert | non directory file</td><td>success or wait</td><td>1</td><td>406036</td><td>CreateFileW</td></tr>
</table>

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\nsw48CC.tmp	success or wait	1	403852	DeleteFileW
C:\Users\user\AppData\Local\Temp\nsc4B5D.tmp	success or wait	1	405C55	DeleteFileW

File Written

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\nsc4B5D.tmp\System.dll</td><td>0</td><td>12288</td><td>4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 71 72 2a fd 35 13 44 fd 35 13 44 fd 35 13 44 fd fd 0f 4a fd 32 13 44 fd 35 13 45 fd 21 13 44 fd fd 1c 19 fd 32 13 44 fd 61 30 74 fd 31 13 44 fd 56 31 6e fd 34 13 44 fd fd 33 40 fd 34 13 44 fd 52 69 63 68 35 13 44 fd 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 19 fd 4f 61 00 00 00 00 00 00 00 00 fd 00 2e 21 0b 01 06 00 00 22 00 00 00 0a 00 00 00 00 00 00 7f 2a 00 00 00 10 00</td><td>MZ@!L!This program cannot be run in DOS mode.$qr*5D5D5DJ2D5E!D2Da0t1DV1n4D3@4DRich5DPELOa.!"*</td><td>success or wait</td><td>1</td><td>4060D6</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\Strepera.wad</td><td>0</td><td>32768</td><td>fd fd fd fd 66 0f 66 fd fd 00 00 00 47 45 07 07 fd fd fd fd fd 7a fd 49 fd 4a 3d 1f 79 6b ca fd fd fd 03 57 5b fd fd fd 6f 12 fd fd 0e 36 02 fd fd fd fd fd 4f 2d 50 fd 6a 22 71 fd fd 68 fd 72 09 fd fd 6d e3 76 fd 16 58 14 fd 08 46 fd 31 fd 42 56 5b fd 70 bc 2c fd 10 2e 1a 54 64 fd 16 1d 4c 7c 63 fd 41 fd 00 5f 43 0f fd fd fd fd 7e fd 37 77 73 fd fd fd 34 7f 5a 0c fd fd 24 fd fd 0b 3e fd fd 65 fd 59 53 82 13 fd 26 fd fd 6c 05 00 00 5f fd fd 0f fd fd fd 00 00 00 fd 1b 0d 7d fd 61 3b 27 61 fd fd 67 2a 59 74 44 4e fd 51 6c fd 60 fd 28 2b 23 3b fd fd fd fd fd 13 25 33 0a fd 2b 5d 04 0f 75 01 18 5c 4b fd 38 fd fd 3c 66 fd 2f fd 29 fd fd 77 fd 30 12 6c 1a fd 3a 6e fd 78 fd 06 4e 74 7b fd 1e 05 fd fd 3f</td><td>ffGEzIJ=ykW[o6O-Pj"qhrmvXF1BVp,.TdL|cA_C~7ws4Z$>eYS&l_}a;'ag*YDNQl`(+#;%3]u\K8<f/)w0l:nxNt{?</td><td>success or wait</td><td>3</td><td>4060D6</td><td>WriteFile</td></tr>
</table>

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\AEGISIIINVHelper.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 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 20 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 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 0f 50 fd fd 4b 31 f8 4b 31 f8 4b 31 f8 42 49 58 fd 47 31 f8 19 59 b9 49 31 f8 51 0c fd 4a 31 f8 19 59 b9 44 31 f8 19 59 f9 43 31 f8 19 59 39 48 31 f8 42 49 4f fd 4a 31 f8 42 49 48 fd 4a 31 f8 38 53 b9 4e 31 f8 4b 31 b8 03 31 f8 fd 58 b9 48 31 f8 fd 58 f9 4a 31 f8 fd 58 34 fd 4a 31 f8 4b 31 5c fd 4a 31 fd	MZ@ !L!This program cannot be run in DOS mode.$PK1K1K1BIXG1YI1J1YD1YC1YH1BIOJ1BIHJ18SN1K11 XH1XJ1X4J1K1\J1	success or wait	2	4060D6	WriteFile
C:\Users\user\AppData\Local\Temp\AsSQLHelper.dll	0	32768	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 01 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 fd 5f fd 25 fd 3e fd 76 fd 3e fd 76 fd 3e fd 76 fd 46 4e 76 fd 3e fd 76 fd 5c fd 77 fd 3e fd 76 fd 56 fd 77 fd 3e fd 76 fd 56 fd 77 fd 3e fd 76 fd 56 fd 77 fd 3e fd 76 fd 56 fd 77 fd 3e fd 76 13 60 fd 77 fd 3e fd 76 fd 3e fd 76 fd 3e fd 76 21 57 fd 77 fd 3e fd 76 21 57 fd 77 fd 3e fd 76 21 57 22 76 fd 3e fd 76 fd 3e 4a 76 fd 3e fd 76 21 57 fd 77 fd 3e fd 76 52 69 63 68 fd 3e fd	MZ@!L!This program cannot be run in DOS mode.$_%>v>v>vFNv>v\w>vVw>vVw>vVw>vVw>v`w>v>v>v!Ww>v!Ww>v!W"v>v>Jv>v!Ww>vRich>	success or wait	2	4060D6	WriteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\CoverDes.exe.manifest	0	1070	ff 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 38 22 20 73 74 61 6e 64 61 6c 6f 6e 65 3d 22 79 65 73 22 20 3f 3e 0d 0a 3c 61 73 73 65 6d 62 6c 79 20 78 6d 6c 6e 73 3d 22 75 72 6e 3a 73 63 68 65 6d 61 73 2d 6d 69 63 72 6f 73 6f 66 74 2d 63 6f 6d 3a 61 73 6d 2e 76 31 22 20 6d 61 6e 69 66 65 73 74 56 65 72 73 69 6f 6e 3d 22 31 2e 30 22 3e 0d 0a 20 20 20 20 3c 64 65 70 65 6e 64 65 6e 63 79 3e 0d 0a 20 20 20 20 20 20 20 3c 64 65 70 65 6e 64 65 6e 74 41 73 73 65 6d 62 6c 79 3e 0d 0a 20 20 20 20 20 20 20 20 20 20 20 3c 61 73 73 65 6d 62 6c 79 49 64 65 6e 74 69 74 79 20 74 79 70 65 3d 22 77 69 6e 33 32 22 20 6e 61 6d 65 3d 22 4d 69 63 72 6f 73 6f 66 74 2e 57 69 6e 64 6f 77 73 2e 43 6f 6d 6d 6f	<?xml version="1.0" encoding="UTF-8" standalone="yes" ?><assembly xmlns="urn:schemas-microsoft-com:asm.v1" manifestVersion="1.0"> <dependency> <dependentAssembly> <assemblyIdentity type="win32" name="Microsoft.Windows.Commo	success or wait	1	4060D6	WriteFile
C:\Users\user\AppData\Local\Temp\emblem-default-symbolic.symbolic.png	0	288	fd 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 10 00 00 00 10 08 06 00 00 00 1f fd fd 61 00 00 00 04 73 42 49 54 08 08 08 08 7c 08 64 fd 00 00 00 fd 49 44 41 54 38 fd fd fd 4e 02 51 10 fd fd 27 fd fd fd 09 fd 58 fd 73 01 5e fd 06 2f 48 fd 66 fd 15 13 fd fd 42 4a fd 09 fd 01 56 5b fd 62 fd fd 71 73 76 41 13 fd 64 fd 5c 79 fd 39 3f fd fd fd 7a fd 60 fd 2f 14 fd fd 0e 27 fd fd 5b fd 51 fd fd 27 fd fd fd 4d 07 fd fd 0d f9 6d 77 75 4e fd 5c fd fd 1f fd 68 fd fd 28 7c fd 03 fd fd 10 0d fd fd 70 fd 4b 0c fd 49 fd 25 fd fd 05 fd fd 20 fd fd 2a fd 06 78 fd 74 7e fd 6b 57 fd 60 56 27 fd 38 fd 57 fd 4b fd 6c fd 34 0e 0b 39 fd 26 5c fd 06 6b fd fd 33 46 fd 1c fd fd fd 91 fd fd 34 fd 30 03 6f 70 fd 72 4c 23 fd fd fd b2 0b 4e 3a fd	PNGIHDRasBIT|dIDAT8 NQ'Xs^/HfBJ V[bqsvAdy9? z`/'[Q'MmwuN\h(|pKI% *xt~kW`V'8WKI49&\k3F4 0oprL#N:	success or wait	1	4060D6	WriteFile

<table>
<tr><th>File Path</th><th>Offset</th><th>Length</th><th>Value</th><th>Ascii</th><th>Completion</th><th>Count</th><th>Source Address</th><th>Symbol</th></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\face-crying.png</td><td>0</td><td>893</td><td>fd 50 4e 47 0d 0a 1a 0a
00 00 00 0d 49 48 44 52
00 00 00 10 00 00 00 10
08 06 00 00 00 1f fd fd 61
00 00 03 44 49 44 41 54
78 01 65 fd 43 fd fd 48 00
46 5f fd fd 74 7a 6c 7b 6d
f6 6d f6 6d 36 6d fd 1e 3b
3d 46 2b fd fd 6a fd fd fd
fd 5e fd fd 72 e9 fd 11 09
0f fd 19 fd fd 68 5a fd 04
0c 25 53 6e fd fd fd 5a fd
fd fd fd 7c 67 fd 7f fd 6f fd
63 fd fd 66 fd b1 6b fd fd
23 fd 59 fd 35 b8 fd 32 fd
fd fd 72 34 34 fd 74 1a fd
fd 5b 7c fd 45 57 10 fd fd
fd 45 fd fd 33 76 7f fd fd
fd 6f fd fd 17 6e 18 19 fd
79 fd 56 fd 25 fd 5c 67 fd
5d fd 58 59 12 29 fd 50
51 17 fd 68 7e 0c 4d 75
12 3a 49 fd 7e fd 21 7b
64 74 fd fd fd 2d 7f fd fd
00 63 19 fd fd fd fd fd 1b
fd 7e fd 69 68 73 fd 0f 3c
fd 32 33 68 fd 71 fd fd 04
41 41 fd fd fd fd</td><td>PNGIHDRaDIDATxeCHF
_tzl{mmmm;=F
+jrhZ%SnZ|gocfk#Y52r4
4t[|EWE3v
onyV%\g]XY)PQh~Mu:I~!
{dt-c~ihs<23hqAA</td><td>success or wait</td><td>1</td><td>4060D6</td><td>WriteFile</td></tr>
<tr><td>C:\Users\user\AppData\Local\Temp\wxbase30u_xml_gcc_custom.dll</td><td>0</td><td>32768</td><td>4d 5a fd 00 03 00 00 00
04 00 00 00 fd fd 00 00 fd
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 fd 00 00 00 0e
1f fd 0e 00 fd 09 fd 21 fd
01 4c fd 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 64 fd 0c 00 00 00
00 00 00 00 00 00 00 00
00 00 fd 00 2e 22 0b 02
02 23 00 42 02 00 00 1e
03 00 00 02 00 00 50 13
00 00 00 10 00 00 00 00
1c 64 00 00 00 00 00 10
00 00 00 02 00 00 04 00
00 00 00 00 00 00 05 00
02 00 00 00 00 00 00 fd
03 00 00 04 00 00 32 fd
03 00 03 00 60 01 00 00
20 00 00 00 00 00 00 10
00 00 00 00 00 00 00 00
10 00 00 00 00 00 00 10
00 00 00 00 00</td><td>MZ@!L!This program
cannot be run in DOS
mode.$PEd."#BPd2`</td><td>success or wait</td><td>7</td><td>4060D6</td><td>WriteFile</td></tr>
</table>

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\aSsc9zh1ex.exe	unknown	512	success or wait	249	4060A7	ReadFile
C:\Users\user\Desktop\aSsc9zh1ex.exe	unknown	4	success or wait	2	4060A7	ReadFile
C:\Users\user\Desktop\aSsc9zh1ex.exe	unknown	4	success or wait	26	4060A7	ReadFile
C:\Users\user\AppData\Local\Temp\Strepera.wad	unknown	77432	success or wait	1	732D2C59	ReadFile

Disassembly

No disassembly