ID: 679607
Sample Name: loader.exe
Cookbook: default.jbs
Time: 04:27:07
Date: 06/08/2022
Version: 35.0.0 Citrine

Table of Contents

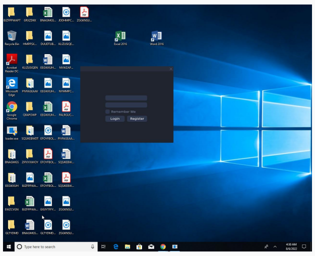
Windows Analysis Report

loader.exe

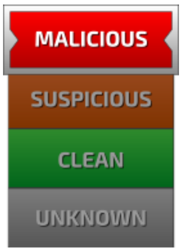
Overview

General Information

Sample Name:	loader.exe
Analysis ID:	679607
MD5:	e5fd705d3e71f83.
SHA1:	551751a4e05ddc..
SHA256:	557caa9cc31a83..
Tags:	exe
Infos:	



Detection

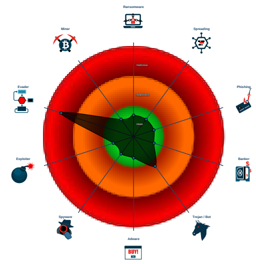


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Hides threads from debuggers
- Overwrites code with unconditional j…
- Tries to evade analysis by executio…
- Tries to detect virtualization through…
- Tries to detect sandboxes and other…
- Tries to detect debuggers (CloseHan…
- PE file contains section with specia…
- Found a high number of Window / U…
- AV process strings found (often use…
- May sleep (evasive loops) to hinder…
- Detected TCP or UDP traffic on non…

Classification



Process Tree

- **System is w10x64**
- loader.exe (PID: 5972 cmdline: "C:\Users\user\Desktop\loader.exe" MD5: E5FD705D3E71F8305FA11E8D1CD2984E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

System Summary

PE file contains section with special chars

Hooking and other Techniques for Hiding and Protection

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion

Tries to evade analysis by execution special instruction (VM detection)

Tries to detect virtualization through RDTSC time measurements

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

Anti Debugging

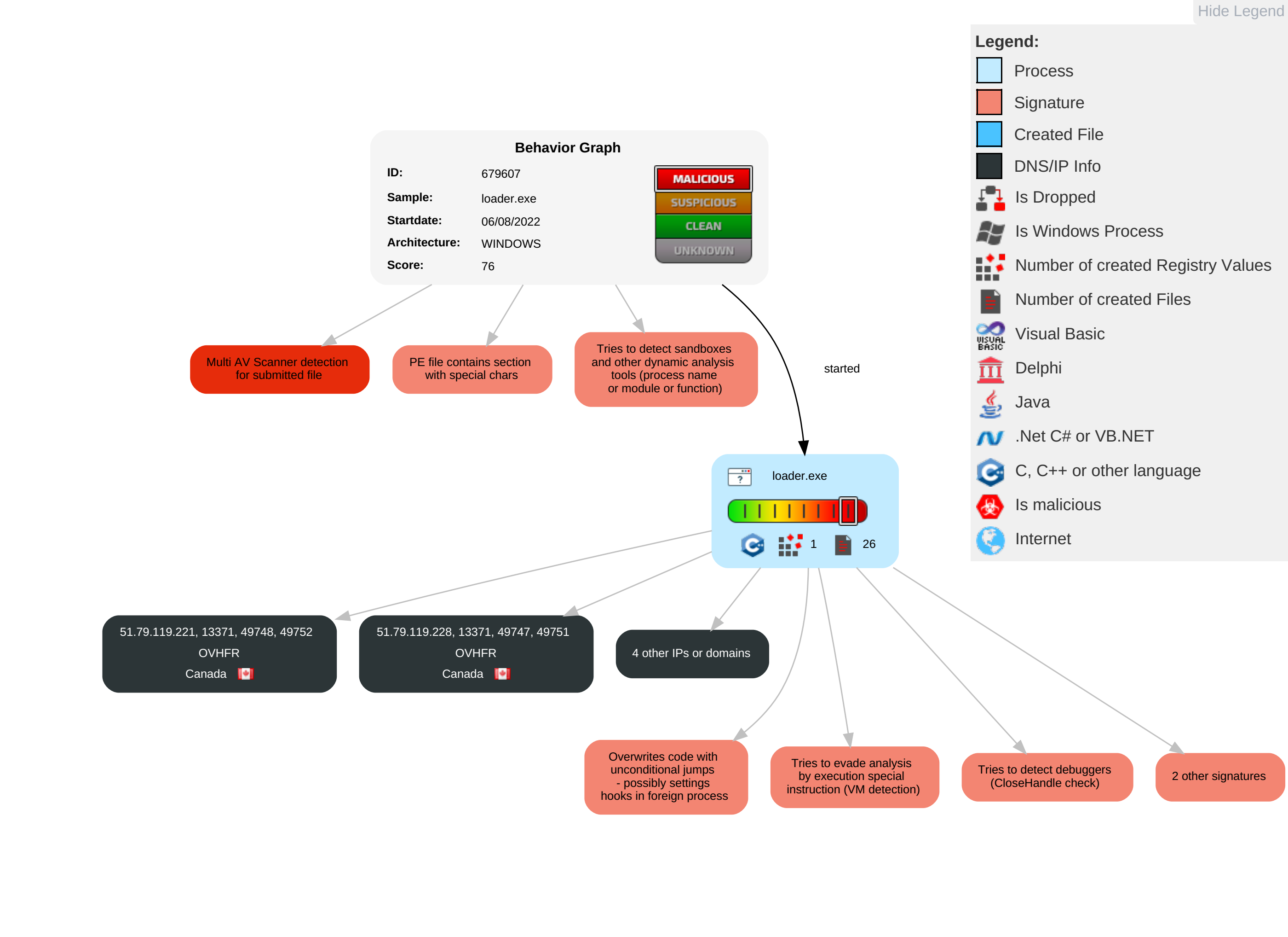
Hides threads from debuggers

Tries to detect debuggers (CloseHandle check)

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	Windows Management Instrumentation	Path Interception	Path Interception	1 Masquerading	1 Credential API Hooking	1 Query Registry	Remote Services	1 Credential API Hooking	Exfiltration Over Other Network Medium	1 Non-Standard Port	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 4 Virtualization/Sandbox Evasion	LSASS Memory	5 4 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	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 4 Virtualization/Sandbox Evasion	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
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	2 1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

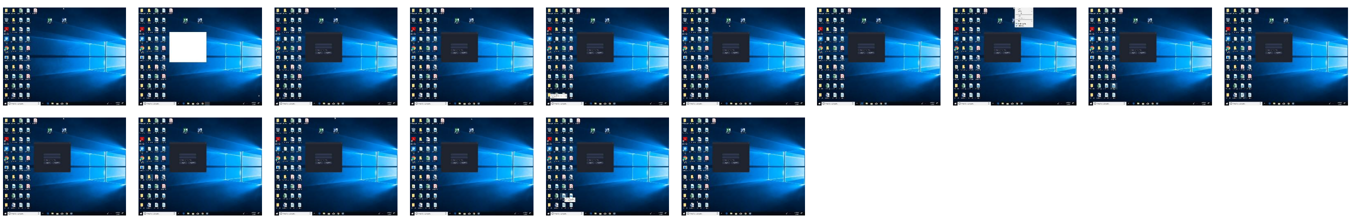
Behavior Graph



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
loader.exe	23%	Virustotal		Browse
loader.exe	17%	Metadefender		Browse
loader.exe	46%	ReversingLabs	Win64.Trojan.Phonzy	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

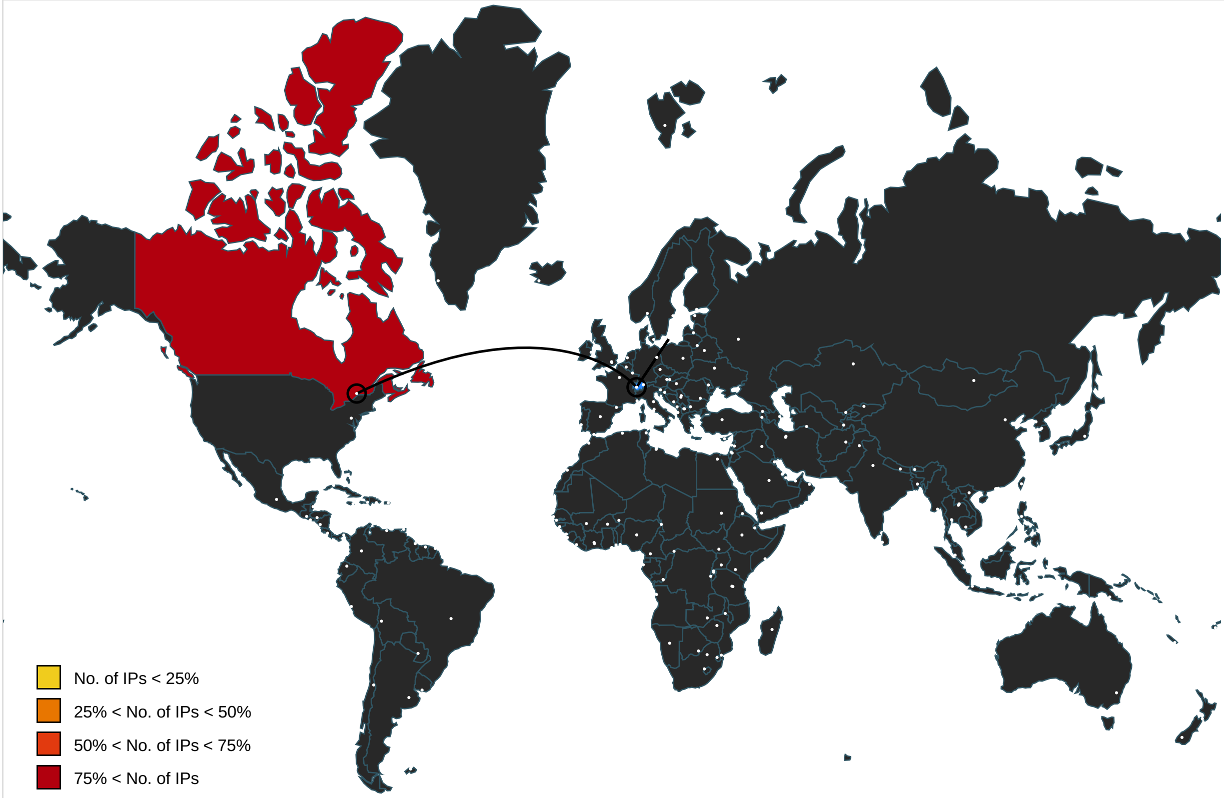
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.79.119.229	unknown	Canada		16276	OVHFR	false
51.79.119.228	unknown	Canada		16276	OVHFR	false
51.79.119.221	unknown	Canada		16276	OVHFR	false
51.79.119.230	unknown	Canada		16276	OVHFR	false
51.79.119.231	unknown	Canada		16276	OVHFR	false

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	679607
Start date and time: 06/08/202204:27:07	2022-08-06 04:27:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	loader.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:	25
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:	mal76.evad.winEXE@1/4@0/6
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information.
- TCP Packets have been reduced to 100
- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 8.248.147.254, 8.248.115.254, 8.241.126.121, 8.253.95.120, 67.26.81.254, 173.222.108.210, 173.222.108.226
- Excluded domains from analysis (whitelisted): www.bing.com, fg.download.windowsupdate.com.c.footprint.net, fs.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, a767.dspw65.akamai.net, arc.msn.com, wu-bg-shim.trafficmanager.net, download.windowsupdate.com.edgesuite.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
04:28:15	API Interceptor	1x Sleep call for process: loader.exe modified

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:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\f83f6d5d89b61b17f0d3863070323a34_d06ed635-68f6-4e9a-955c-4899f5f57b9a

Process:	C:\Users\user\Desktop\loader.exe
File Type:	data
Category:	dropped
Size (bytes):	2249
Entropy (8bit):	7.644646383207026
Encrypted:	false
SSDEEP:	48:4o/OwVUqbMxLUFq8g5bnF3RoIofFCRI2fqBaj:4o/tjbMx4cbnFhJWs8Baj
MD5:	F34CC48D39D75F0E8170A85E925F085F
SHA1:	9CB613D56269FD8420EAD7ADE1B1E064315334AF
SHA-256:	9B52B1D4D6CB0C7332A884F7DE4D52ADA49B71213359D0A0A5DC755187FABE51
SHA-512:	1088C204A04A1B7E565CFBF49A261478DA98B586DDFBCD15785DFC84654B05F5226E6C1EB0FE0EFC15725C34930D8E87D535659E140134BD41335F1B3A1365D
Malicious:	false
Reputation:	low
Preview:	........%.......P......................95505749-1328-4162-b38a-e051b523ca17....................RSA1...............%....F...:Ry...g.......pz..L......a...nu.....{.....,.'......}..I....3.6R..3....... .....K.7%].].N.8`F.sYv.W..t.$R...a.#..K...m..I..W..8T.$.u.<.6.lG.q...&.D.......3.D.._..a.&<.L.5K....Oo.;,..oNkLV....2N.;....C..U..V#...2..}_..4.E.^.._.$....s.......................z..O... ...X......L...5...y....,...C.r.y.p.t.o.A.P.I. .P.r.i.v.a.t.e. .K.e.y....f...... ....F.5.G.........B..m..C...S............. ....d.&......@t..].R..0..I...a. iAP.........{..55..<~.......%]....B...j.......+..m\| \....GR..JLP.Z!..B7).aT..\m.o.s....V.........j..E.b...k.Cz...i`.p......4q.=.st.h..f.[yW..jNnkU34..W..pU...g&(..v.Q0\|...V..G..d^...$..u[...w.......9`.p...x.....7D...M..R.....Et..U.`...:z..#.: =..q.4...........0G..@...`.ET4..i.,.._.....B.J=.X0^n.79..;.U..}9......V.........I.!W.'r........\.7....*.O,..wis.........}......C.G.KF|.&.!.L.rU.v...R?<.....zK

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\loader.exe
File Type:	Microsoft Cabinet archive data, 61712 bytes, 1 file
Category:	dropped
Size (bytes):	61712
Entropy (8bit):	**7.995044632446497**
Encrypted:	**true**
SSDEEP:	1536:gzjJiDImMsrjCtGLaexX/zL09mX/lZHIxs:gPJiDI/sr0Hexv/0S/zx
MD5:	589C442FC7A0C70DCA927115A700D41E
SHA1:	66A07DACE3AFBFD1AA07A47E6875BEAB62C4BB31
SHA-256:	2E5CB72E9EB43BAAFB6C6BFCC573AAC92F49A8064C483F9D378A9E8E781A526A
SHA-512:	1B5FA79E52BE495C42CF49618441FB7012E28C02E7A08A91DA9213DB3AB810F0E83485BC1DD5F625A47D0BA7CFCDD5EA50ACC9A8DCEBB39F048C40F01E941 55B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF............,...................I........y.........Tf. .authroot.stl..W.`.4..CK..8U[...q.yL'sf!d.D..."2.2g.<dVI.!.....$).\...!2s..(...[.T7..{}...g....g.....w.km$.&|..qe.n.8+..&...O...`...+..C..... .`h!0.I.(C..1Q*L.p..".s..B.....H......fUP@..5...(X#.t.2lX.>.y|D.0Z0...M....I(.#.-... ...(.J....2..`.hO..{l+.bd7y.j..u.....3....<......3....s.T...._.'...%{v...s.............KgV.0..X=.A.9w9.Ea.x....... ...\.=.e.C2......9.......`.o... .......@pm.. a.....-M.....{...s.mW.....;.+...A......0.g..L9#.v.&O>./xSH.S.....GH.6.j...`2.(0g..... Lt........h4.iQ?....[.K.....uI......}.....d....M.....6q.Q~.0.\.'U^)`. .u.....-........d..7...2.-.2+3.....A./.%Q...k...Q.,...H.B.%..O..x..5\...Hk.......B.';"Ym.'....X.l.E.6..a8.6..nq..x.r4..1t.....,..u.O..O.L...Uf...X.u.F .(.(....."..q...n{%U.-u....l6!....Z....~o0.}Q'.s.i ....7...>4x...A.h.Mk].O.z.].6...53...b^;..>e..x.'1..\p.O.k..B1w..|..K.R.....2.e0..X.^...I...w..!.v5B]x..z.6.G^uF..].b.W...'..I.;..p..@L{.E..@W..3.&...

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Users\user\Desktop\loader.exe
File Type:	data
Category:	modified
Size (bytes):	326
Entropy (8bit):	3.1297566246827087
Encrypted:	false
SSDEEP:	6:kKI+N+SkQlPlEGYRMY9z+4KlDA3RUeWlEZ21:wNkPlE99SNxAhUeE1
MD5:	FBDB41C5DDAACA78BA5ECB1A0BEE5640
SHA1:	BC8BFC1D376958D61439422930850CD5F69F1805
SHA-256:	7D4BB9D9E727895C6EEA59FEA9C766799C120402D5490FA31831D1CF6CA4CE0C

SHA-512:	9AAB9746189C9A8B4B396BA2D825AEFDECAA68BD06943F6A7326978531C8F7B0BBE87B0CB995FFB30C65B7B93B74923AA94511FB88E3D91F907C9F3DCAB4DA03
Malicious:	false
Reputation:	low
Preview:	p...... ....v.....(.. ....L.........$..............h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./. s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.9.f.4.c.9.6.9.8.b.d.8.1.:.0."...

C:\Users\user\AppData\Roaming\Microsoft\SystemCertificates\My\Certificates\6D57A09278E9D03E442F152BE212C307E8475812

Process:	C:\Users\user\Desktop\loader.exe
File Type:	data
Category:	dropped
Size (bytes):	980
Entropy (8bit):	6.899463213878604
Encrypted:	false
SSDEEP:	24:8AgmQpZduzlC4bYs6PhUBoo2t7KKyNLcR9mMdmgmmCZwghn:819UoaJyWWlKKwIdX3E1n
MD5:	D38C7B9090AE1D5DC15821B44650C7AB
SHA1:	0AD315F5327304EE4E03D77DA8B67BDF9B076D9D
SHA-256:	1FB5BD89E9CE594F0B266F4B43B008A8DF122A139FD1F77379BE5FF6601F221F
SHA-512:	1C0594BC6F926BBDFAC00421AF11568EE2C69BCF2ECBC4EEA760757B6006B557DCAAEA25656F198C28C542D952653E7D06A60E12AD82A4D1870828A3522A23F
Malicious:	false
Reputation:	low
Preview:	.................*....."..l..3............d.d.d.d.d..............m.i.c.r.o.s.o.f.t..............0...+..............l.............. ....9.5.5.0.5.7.4.9.-.1.3.2.8.-.4.1.6.2.-.b.3.8.a.-.e.0.5.1.b.5.2.3.c.a.1 .7....................mW..x..>D/.+.....GX. ....0...0.........f./V...B......10...*.H........0.1.0...U....user at 4245050...220806112813Z..270806112813Z0.1.0...U....user at 4245050.." 0...*.H............0............s....$._.^.E.4._}..2..#V..U..C....;.N2....VLkNo..,;.oO...K5.L.<&.a._..D.3.......D.&...q.Gl.6.<.u.$.T8..W..I..m...K..#.a..R$.t..W.vYs.F`8.N..].]%7.K........ ...3..R6.3.....l..}......'..,....{.....un...a.......L...zp.......g...yR:...F....%.....0...*.H............8.....g..k..'.Tar....F..L.'...u'...~g.A...<...Q.x.`!,..;..{..{..+..w..p..-.$.Z..}8,T....Hj........O0vyn[.'..xi_.H.k.|r.U.=j1.U .Ew.t..y.v.'...LC.............~.2.4E<9.^.#.......-..k6.E.sVx..",.z...'..f.j..v..1....I}z!..:.G..H.E|.8JC{;...|.

Static File Info

General

File type:	PE32+ executable (GUI) x86-64, for MS Windows
Entropy (8bit):	7.956098799743011
TrID:	• Win64 Executable GUI (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	loader.exe
File size:	9042944
MD5:	e5fd705d3e71f8305fa11e8d1cd2984e
SHA1:	551751a4e05ddc9fb3fc3989d50032c15b99caf9
SHA256:	557caa9cc31a834b807583b61c2b81a001962cd85419616c0f297d0c84b29d21
SHA512:	5b20a5ffe995f76f99714d9b0cce3e3a85f4b71440a76138039e6bf9854c08da0adbe6a3c08cead1bcb67c5302419574cef8c5ca87c3eab34a5f02c3a5311b0c
SSDEEP:	196608:Vs1m7bBPEAUdZzfjBDZ9AU84V0zFyWv6AJ5ypqetZ9j1:VWmh1YPBDZ9AnFCyNIfj1
TLSH:	A39623EFA1103768C01EC4345823BD49B1F6962E1EF88A6AB5DF7AC06F6E811D542F47
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..d....k.b..........#......v...&.......B.........@... ....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x140f54281
Entrypoint Section:	w^]>
Digitally signed:	false

Imagebase:	0x140000000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x62E46B1F [Fri Jul 29 23:19:59 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	15fd01fb7e6ca57c8d5b667e1bfac6f6

Entrypoint Preview

Instruction
push 69D78D6Dh
call 00007FB2D101DC7Fh
sub dword ptr [ebx-5D758BD8h], eax
or bl, ah
retf
wait
ret
or al, dl
or ecx, dword ptr [F425F3B7h]
movsd
mov byte ptr [edx], dl
and eax, 59B480F4h
fmulp st(3), st(0)
jmp far FBF8h : 74239330h
and ch, dl
retf
outsb
xchg eax, edx
adc al, FFFFFF8Bh
daa
push esp
das
sub dh, byte ptr [esi+ebp+742F3B55h]
xor eax, D334260Fh
sbb ah, byte ptr [esi]
ror ebx, 1
inc eax
wait
and al, DDh
or edi, dword ptr [edi+17F428DFh]
mov eax, 89F4283Eh
fdiv qword ptr [ebp-2Dh]
retf
mov al, byte ptr [742EBFF8h]
sbb byte ptr [ebx], bh
or al, D8h
retf
adc eax, 8BDDAC8Ah
cmpsb
mov bl, 37h
xchg dword ptr [edi+1Eh], esp
adc al, B3h
jns 00007FB2D0EBF82Ah

Instruction
xchg eax, esp
push esi
adc dword ptr [edi-34068A59h], 0000A319h
push ebx
cwde
int 63h
mov ebp, BF44FEFAh
movsd
adc dword ptr [edi-2031AE10h], 65CF94F8h
pop eax
call 00007FB337BC01DFh
jnp 00007FB2D0EBF775h
insd
sub byte ptr [ebx+4F849E82h], ah
mov al, 2Eh
stosd
popfd
push ebp
aaa
mov edi, 2412C97Ah
inc ecx
movsb
sar ah, 1
push edi

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x93f5b8	0xc4f	w^]>
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf167b0	0x2f8	w^]>
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x110e000	0x2e1	h`J?
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x10fc9e0	0x10a10	w^]>
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	0x966b30	0x48	w^]>
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x10fc8a0	0x138	w^]>
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x959000	0x2b0	w^]>
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
4uN%	0x1000	0xe74fe	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
A]zn	0xe9000	0x7ff6a	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
+/*9	0x169000	0xc4150	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
'x00	0x22e000	0xda7c	0x0	False	0	empty	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
'IAL	0x23c000	0x631241	0x0	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
w^]>	0x86e000	0x89f3f0	0x89f400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_CODE, IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_NOT_PAGED, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
h`J?	0x110e000	0x2e1	0x400	False	0.4013671875	data	4.307570076268581	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x110e058	0x289	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	Wow64DisableWow64FsRedirection
USER32.dll	ShowWindow
GDI32.dll	DeleteObject
ADVAPI32.dll	RegSetKeyValueA
SHELL32.dll	SHGetKnownFolderPath
ole32.dll	CoCreateGuid
OLEAUT32.dll	VariantClear
ntdll.dll	NtSuspendThread
MSVCP140.dll	?_Getcat@?$codecvt@DDU_Mbstatet@@@std@@SA_KPEAPEBVfacet@locale@2@PEBV42@@Z
SHLWAPI.dll	PathRemoveFileSpecA
IMM32.dll	ImmSetCompositionWindow
WS2_32.dll	WSAGetLastError
CRYPT32.dll	CertAddCertificateContextToStore
Secur32.dll	InitSecurityInterfaceW
d3d11.dll	D3D11CreateDeviceAndSwapChain
D3DCOMPILER_47.dll	D3DCompile
gdiplus.dll	GdipFree
DNSAPI.dll	DnsNameCompare_W
RPCRT4.dll	UuidCreate
VCRUNTIME140_1.dll	__CxxFrameHandler4
VCRUNTIME140.dll	memmove
api-ms-win-crt-heap-l1-1-0.dll	_set_new_mode
api-ms-win-crt-runtime-l1-1-0.dll	_errno
api-ms-win-crt-stdio-l1-1-0.dll	_get_stream_buffer_pointers
api-ms-win-crt-string-l1-1-0.dll	isalnum
api-ms-win-crt-utility-l1-1-0.dll	rand
api-ms-win-crt-convert-l1-1-0.dll	strtof
api-ms-win-crt-filesystem-l1-1-0.dll	remove
api-ms-win-crt-time-l1-1-0.dll	_time64
api-ms-win-crt-math-l1-1-0.dll	powf
api-ms-win-crt-environment-l1-1-0.dll	getenv
api-ms-win-crt-locale-l1-1-0.dll	_configthreadlocale
WTSAPI32.dll	WTSSendMessageW
KERNEL32.dll	GetSystemTimeAsFileTime
USER32.dll	GetUserObjectInformationW
KERNEL32.dll	LocalAlloc, LocalFree, GetModuleFileNameW, GetProcessAffinityMask, SetProcessAffinityMask, SetThreadAffinityMask, Sleep, ExitProcess, FreeLibrary, LoadLibraryA, GetModuleHandleA, GetProcAddress
USER32.dll	GetProcessWindowStation, GetUserObjectInformationW

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

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 04:28:13.433515072 CEST	49735	13371	192.168.2.3	51.79.119.230
Aug 6, 2022 04:28:13.433659077 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:13.538110971 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:13.538678885 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:13.539931059 CEST	13371	49735	51.79.119.230	192.168.2.3
Aug 6, 2022 04:28:14.178667068 CEST	49735	13371	192.168.2.3	51.79.119.230
Aug 6, 2022 04:28:14.285240889 CEST	13371	49735	51.79.119.230	192.168.2.3
Aug 6, 2022 04:28:14.631762028 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:14.736622095 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:14.768516064 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:14.788032055 CEST	49735	13371	192.168.2.3	51.79.119.230
Aug 6, 2022 04:28:14.896356106 CEST	13371	49735	51.79.119.230	192.168.2.3
Aug 6, 2022 04:28:14.897473097 CEST	49744	13371	192.168.2.3	51.79.119.229
Aug 6, 2022 04:28:14.933604956 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:15.001610041 CEST	13371	49744	51.79.119.229	192.168.2.3
Aug 6, 2022 04:28:15.002943993 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:15.016450882 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:15.121400118 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:15.334917068 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:15.433712959 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:15.433820963 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:15.678740025 CEST	49744	13371	192.168.2.3	51.79.119.229
Aug 6, 2022 04:28:15.783205032 CEST	13371	49744	51.79.119.229	192.168.2.3
Aug 6, 2022 04:28:16.131970882 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:16.236836910 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:16.288161039 CEST	49744	13371	192.168.2.3	51.79.119.229
Aug 6, 2022 04:28:16.393563986 CEST	13371	49744	51.79.119.229	192.168.2.3
Aug 6, 2022 04:28:16.452487946 CEST	49747	13371	192.168.2.3	51.79.119.228
Aug 6, 2022 04:28:16.559268951 CEST	13371	49747	51.79.119.228	192.168.2.3
Aug 6, 2022 04:28:16.979001999 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:17.086649895 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:17.131998062 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:17.178889036 CEST	49747	13371	192.168.2.3	51.79.119.228
Aug 6, 2022 04:28:17.286429882 CEST	13371	49747	51.79.119.228	192.168.2.3
Aug 6, 2022 04:28:17.301624060 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:17.406037092 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:17.522602081 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:17.788279057 CEST	49747	13371	192.168.2.3	51.79.119.228
Aug 6, 2022 04:28:17.895164013 CEST	13371	49747	51.79.119.228	192.168.2.3
Aug 6, 2022 04:28:17.896352053 CEST	49748	13371	192.168.2.3	51.79.119.221
Aug 6, 2022 04:28:17.994832993 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:18.000715017 CEST	13371	49748	51.79.119.221	192.168.2.3
Aug 6, 2022 04:28:18.152419090 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:18.585171938 CEST	49748	13371	192.168.2.3	51.79.119.221
Aug 6, 2022 04:28:18.689703941 CEST	13371	49748	51.79.119.221	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 6, 2022 04:28:19.282669067 CEST	49748	13371	192.168.2.3	51.79.119.221
Aug 6, 2022 04:28:19.335388899 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:19.387276888 CEST	13371	49748	51.79.119.221	192.168.2.3
Aug 6, 2022 04:28:19.439780951 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:20.522902966 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:20.627474070 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:21.632378101 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:21.736681938 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:22.015671968 CEST	49749	13371	192.168.2.3	51.79.119.230
Aug 6, 2022 04:28:22.124047995 CEST	13371	49749	51.79.119.230	192.168.2.3
Aug 6, 2022 04:28:22.635829926 CEST	49749	13371	192.168.2.3	51.79.119.230
Aug 6, 2022 04:28:22.744920969 CEST	13371	49749	51.79.119.230	192.168.2.3
Aug 6, 2022 04:28:22.835557938 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:22.939927101 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:23.335596085 CEST	49749	13371	192.168.2.3	51.79.119.230
Aug 6, 2022 04:28:23.444709063 CEST	13371	49749	51.79.119.230	192.168.2.3
Aug 6, 2022 04:28:23.811834097 CEST	49750	13371	192.168.2.3	51.79.119.229
Aug 6, 2022 04:28:23.918912888 CEST	13371	49750	51.79.119.229	192.168.2.3
Aug 6, 2022 04:28:24.023243904 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:24.127542019 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:24.492155075 CEST	49750	13371	192.168.2.3	51.79.119.229
Aug 6, 2022 04:28:24.599430084 CEST	13371	49750	51.79.119.229	192.168.2.3
Aug 6, 2022 04:28:25.132746935 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:25.176233053 CEST	49750	13371	192.168.2.3	51.79.119.229
Aug 6, 2022 04:28:25.237627983 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:25.283571959 CEST	13371	49750	51.79.119.229	192.168.2.3
Aug 6, 2022 04:28:25.569619894 CEST	49751	13371	192.168.2.3	51.79.119.228
Aug 6, 2022 04:28:25.672688007 CEST	13371	49751	51.79.119.228	192.168.2.3
Aug 6, 2022 04:28:26.335875034 CEST	49751	13371	192.168.2.3	51.79.119.228
Aug 6, 2022 04:28:26.337289095 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:26.440452099 CEST	13371	49751	51.79.119.228	192.168.2.3
Aug 6, 2022 04:28:26.441461086 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:27.023390055 CEST	49751	13371	192.168.2.3	51.79.119.228
Aug 6, 2022 04:28:27.126451969 CEST	13371	49751	51.79.119.228	192.168.2.3
Aug 6, 2022 04:28:27.242733002 CEST	49752	13371	192.168.2.3	51.79.119.221
Aug 6, 2022 04:28:27.348345995 CEST	13371	49752	51.79.119.221	192.168.2.3
Aug 6, 2022 04:28:27.523454905 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:27.627635002 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:27.992371082 CEST	49752	13371	192.168.2.3	51.79.119.221
Aug 6, 2022 04:28:28.097898960 CEST	13371	49752	51.79.119.221	192.168.2.3
Aug 6, 2022 04:28:28.634192944 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:28.738545895 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:28.789309025 CEST	49752	13371	192.168.2.3	51.79.119.221
Aug 6, 2022 04:28:28.894906998 CEST	13371	49752	51.79.119.221	192.168.2.3
Aug 6, 2022 04:28:29.836213112 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:29.940418959 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:31.023808956 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:31.127978086 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:31.535465956 CEST	49753	13371	192.168.2.3	51.79.119.230
Aug 6, 2022 04:28:31.641992092 CEST	13371	49753	51.79.119.230	192.168.2.3
Aug 6, 2022 04:28:32.133248091 CEST	49734	13371	192.168.2.3	51.79.119.231
Aug 6, 2022 04:28:32.237550020 CEST	13371	49734	51.79.119.231	192.168.2.3
Aug 6, 2022 04:28:32.336344957 CEST	49753	13371	192.168.2.3	51.79.119.230
Aug 6, 2022 04:28:32.444093943 CEST	13371	49753	51.79.119.230	192.168.2.3
Aug 6, 2022 04:28:33.023994923 CEST	49753	13371	192.168.2.3	51.79.119.230

Statistics

No statistics

System Behavior

Analysis Process: loader.exe PID: **5972**, Parent PID: **5332**

General

Target ID:	0
Start time:	04:28:08
Start date:	06/08/2022
Path:	C:\Users\user\Desktop\loader.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\loader.exe"
Imagebase:	0x140000000
File size:	9042944 bytes
MD5 hash:	E5FD705D3E71F8305FA11E8D1CD2984E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly