ID: 403997
Sample Name: ACS route, aircraft cond. req information & doc00710020210501154406 PDF.exe
Cookbook: default.jbs
Time: 16:05:50
Date: 04/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

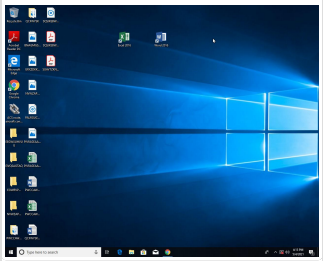
Analysis Report ACS route, aircraft cond. req informatio…

Overview

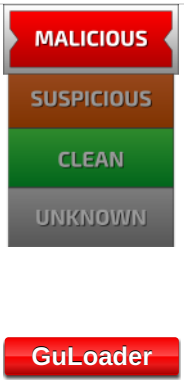
General Information

Sample Name:	ACS route, aircraft cond. req information & doc0071002021050115440 6 PDF.exe
Analysis ID:	403997
MD5:	5777362ea00ed2..
SHA1:	4cbdfa68ef829f9…
SHA256:	f6f23db6c1ecdf6…
Infos:	

Most interesting Screenshot:



Detection

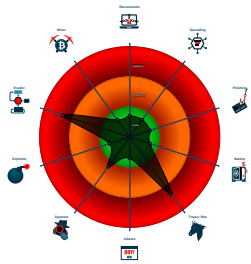


Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- DLL reload attack detected
- Found malware configuration
- Malicious sample detected (through …
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Tries to detect virtualization through…
- Contains functionality for execution …
- Contains functionality to call native f…
- Contains functionality to read the PEB
- PE file contains executable resource…
- Program does not show much activi…
- Queries the volume information (nam…
- Sample file is different than original …
- Uses 32bit PE files

Classification



Startup

- **System is w10x64**
- ACS route, aircraft cond. req information & doc0071002021050115440 6 PDF.exe (PID: 4744 cmdline: 'C:\Users\user\Desktop\ACS route, aircraft cond. req information & doc0071002021050115440 6 PDF.exe' MD5: 5777362EA00ED2DD6C40121450291E7D)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1hJRfPD7mATt1zd_Z0FIM8Q9qnryDNQsL"
}
```

Yara Overview

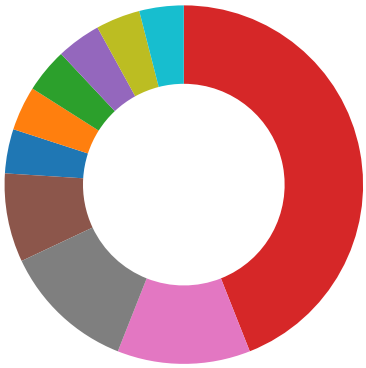
Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.1290771999.0000000002B50000.00000040.00000001.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000000.00000000.204937287.000000000040C000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x110c:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000000.00000002.1285251776.000000000040C000.00000020.00020000.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth	• 0x110c:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Found malware configuration

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Yara detected GuLoader

Hooking and other Techniques for Hiding and Protection:

DLL reload attack detected

Malware Analysis System Evasion:

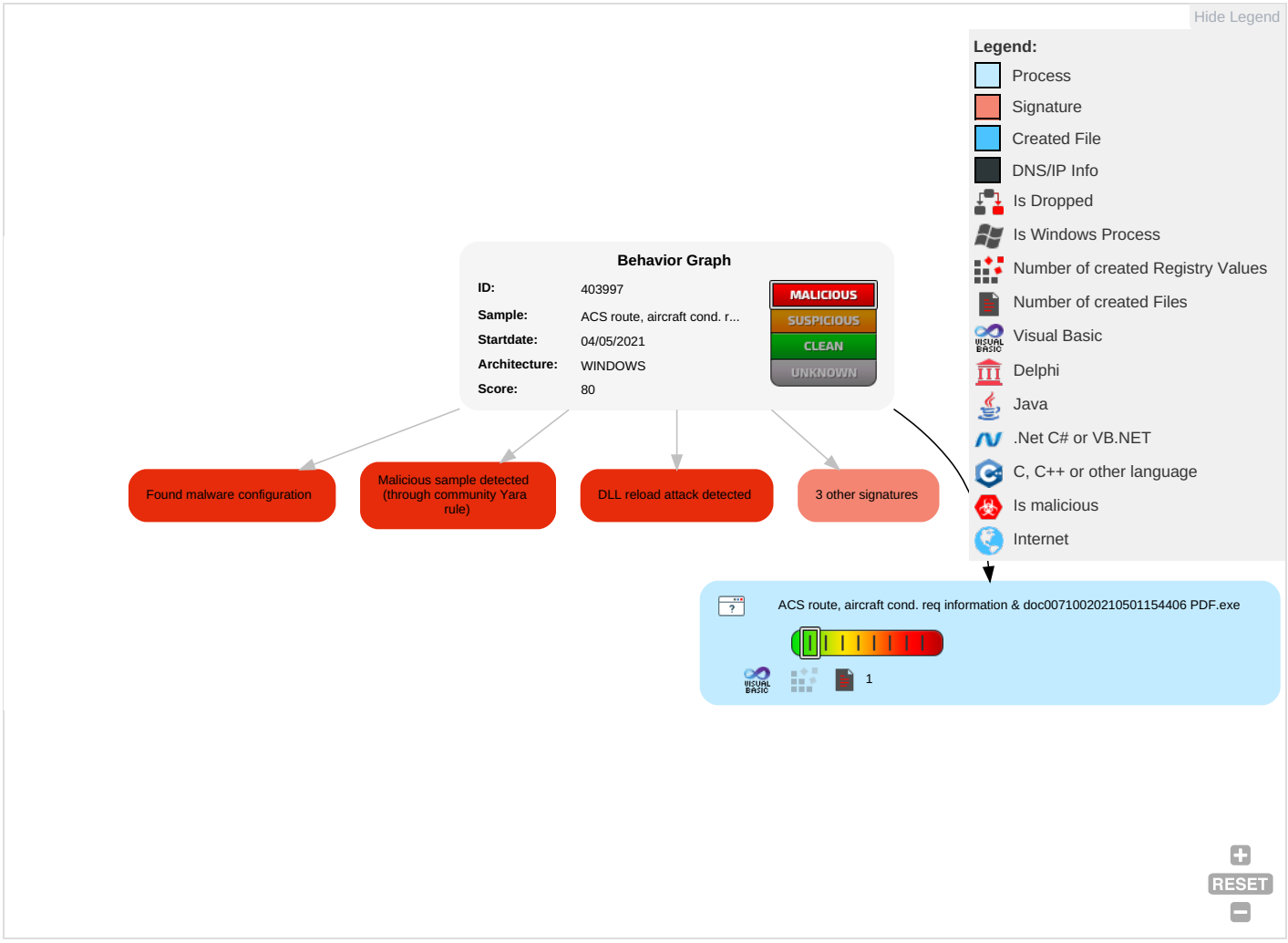
Tries to detect virtualization through RDTSC time measurements

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	In
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 1	Process Injection 1	OS Credential Dumping	Security Software Discovery 1 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	M Sy Pa

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	In
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	DLL Side-Loading 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	D L
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	D D D

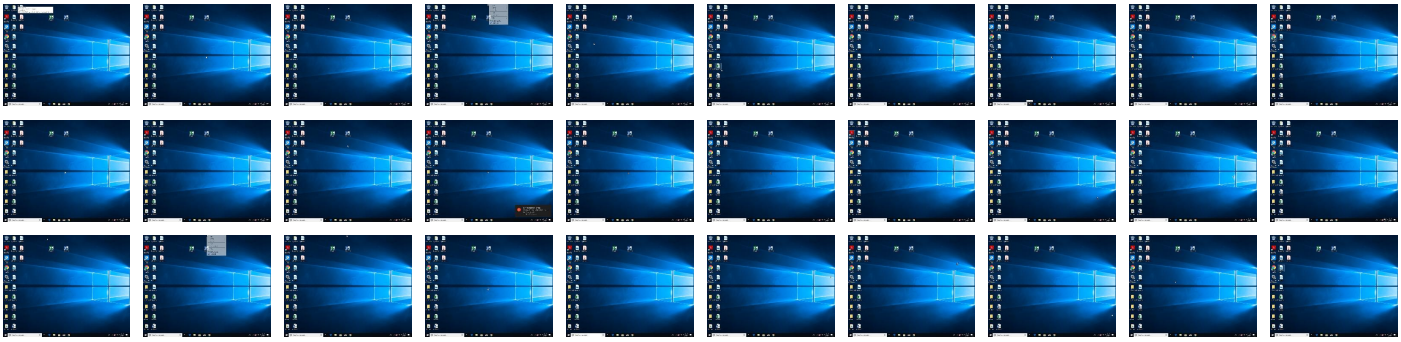
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	403997
Start date:	04.05.2021
Start time:	16:05:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	ACS route, aircraft cond. req information & doc00710020210501154406 PDF.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:	22
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:	mal80.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
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 • Report size getting too big, too many NtAllocateVirtualMemory calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	4.777529017205276
TrID:	• Win32 Executable (generic) a (10002005/4) 99.15% • Win32 Executable Microsoft Visual Basic 6 (82127/2) 0.81% • 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:	ACS route, aircraft cond. req information & doc00710020210501154406 PDF.exe
File size:	98304
MD5:	5777362ea00ed2dd6c40121450291e7d
SHA1:	4cbdfa68ef829f9709ee74bb883985d8a18c4048
SHA256:	f6f23db6c1ecdf6b5766a22434e7a9c24585ecf94cf8a784f1a15640d0f0ba45
SHA512:	b040be11572cb05338212e73492d475211f24c79be94486ada0a5d4438d436bd24e92479d001531dcb6f56045a6901ab5526c72b9dee968e24f8e4a0380d4014
SSDEEP:	1536:OR02SmQFaUvIZddDGaz24YxUzAoma3vx:OnrsaXdZG1409ovJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L.....W.....P... .....|.....`....@.....

File Icon

Icon Hash:	b074cecec891b2e4

Static PE Info

General

Entrypoint:	0x40157c
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:	
Time Stamp:	0x5711B91D [Sat Apr 16 04:01:33 2016 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:	631ffe9ad0b821781f48149fabda62f6

Entrypoint Preview

Instruction
push 0040CA8Ch
call 00007F0480BA7975h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
xor byte ptr [eax], al
add byte ptr [eax], al
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
mov dh, 80h
leave
leave
retf
salc
clc
dec edi
call far 49E6h : 708BCD81h
fild word ptr [eax]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax+edx*2+72h], bl
outsd
push 00000065h
outsb
popad
outsb
jnc 00007F0480BA7983h
add byte ptr [eax], al
add byte ptr [eax], al
dec esp

Instruction
xor dword ptr [eax], eax
sub byte ptr [esi+0B9DFADDh], ah
sal edx, 1
dec ecx
stosb
sub eax, 8D5E5938h
jnle 00007F0480BA79F7h
aad 85h
and cl, ch
mov ecx, AA4E556Bh
test eax, 87B2E630h
or dword ptr [edx], esp
cmp cl, byte ptr [edi-53h]
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
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
mov dh, B3h
add byte ptr [eax], al
push esp
add al, byte ptr [eax]
add byte ptr [eax], al
or dword ptr [eax], eax
jbe 00007F0480BA79EBh
outsb
imul esp, dword ptr [ebp+74h], 73h
jc 00007F0480BA79E3h
add byte ptr [6B000901h], cl
outsd
push 0000006Fh
insd
jc 00007983h
sbb dword ptr [ecx], eax
add byte ptr [edx+00h], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x14ed4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x5a4	.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	

Name	Virtual Address	Virtual Size	Is in Section
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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x10c	.text
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	0x14350	0x15000	False	0.341331845238	data	5.21336422112	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x16000	0xad4	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x5a4	0x1000	False	0.182861328125	data	1.71064501623	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x173bc	0x1e8	data		
RT_GROUP_ICON	0x173a8	0x14	data		
RT_VERSION	0x170f0	0x2b8	COM executable for DOS	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaI4Var, __vbaStrToAnsi, __vbaFpI4, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	PHILAD
FileVersion	1.00
CompanyName	Mummys Technology
Comments	Mummys Technology
ProductName	Mummys Technology
ProductVersion	1.00
FileDescription	Mummys Technology
OriginalFilename	PHILAD.exe

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: ACS route, aircraft cond. req information & doc00710020210501154406 PDF.exe PID: 4744 Parent PID: 5584

General

Start time:	16:06:39
Start date:	04/05/2021
Path:	C:\Users\user\Desktop\ACS route, aircraft cond. req information & doc00710020210501154406 PDF.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\ACS route, aircraft cond. req information & doc0071002021 0501154406 PDF.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	5777362EA00ED2DD6C40121450291E7D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000000.00000002.1290771999.0000000002B50000.00000040.00000001.sdmp, Author: Joe Security • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000000.204937287.000000000040C000.00000020.00020000.sdmp, Author: Florian Roth • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.1285251776.000000000040C000.00000020.00020000.sdmp, Author: Florian Roth
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis