ID: 393904
Sample Name:
samtidshistoriker.exe
Cookbook: default.jbs
Time: 21:47:49
Date: 20/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report samtidshistoriker.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
Data Obfuscation: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Mitre Att&ck Matrix 5
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 7
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 10
Data Directories 12
Sections 12
Resources 12
Imports 12
Version Infos 12
Possible Origin 12
Network Behavior 13
Code Manipulations 13

Statistics 13
System Behavior 13
Analysis Process: samtidshistoriker.exe PID: 5740 Parent PID: 5692 13
General 13
File Activities 13
Disassembly 13
Code Analysis 13

Copyright Joe Security LLC 2021

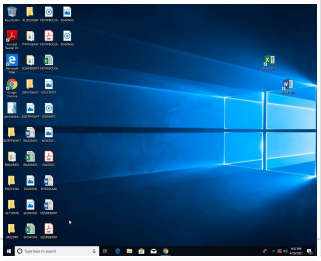
Analysis Report samtidshistoriker.exe

Overview

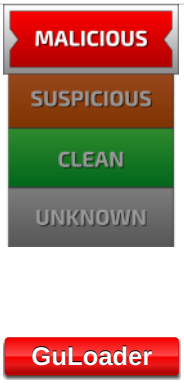
General Information

Sample Name:	samtidshistoriker.exe
Analysis ID:	393904
MD5:	780254149cfe37c..
SHA1:	c28ac373e62a87..
SHA256:	74c9a0f54acec0d..
Infos:	

Most interesting Screenshot:



Detection

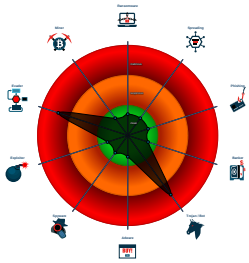


Score:	92
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Found potential string decryption / a…

Classification



Startup

- **System is w10x64**
- samtidshistoriker.exe (PID: 5740 cmdline: 'C:\Users\user\Desktop\samtidshistoriker.exe' MD5: 780254149CFE37CE295A82588BE31204)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=14HidX9PYpF9MdDuU2Alpazy_Sg8A9xmd",
  "Injection Process": [
    "RegAsm.exe",
    "RegSvcs.exe",
    "MSBuild.exe"
  ]
}
```

Yara Overview

Memory Dumps

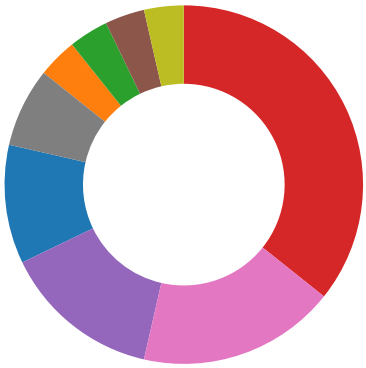
Source	Rule	Description	Author	Strings
00000000.00000002.742722854.000000000500000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: samtidshistoriker.exe PID: 5740	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: samtidshistoriker.exe PID: 5740	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Copyright Joe Security LLC 2021

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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

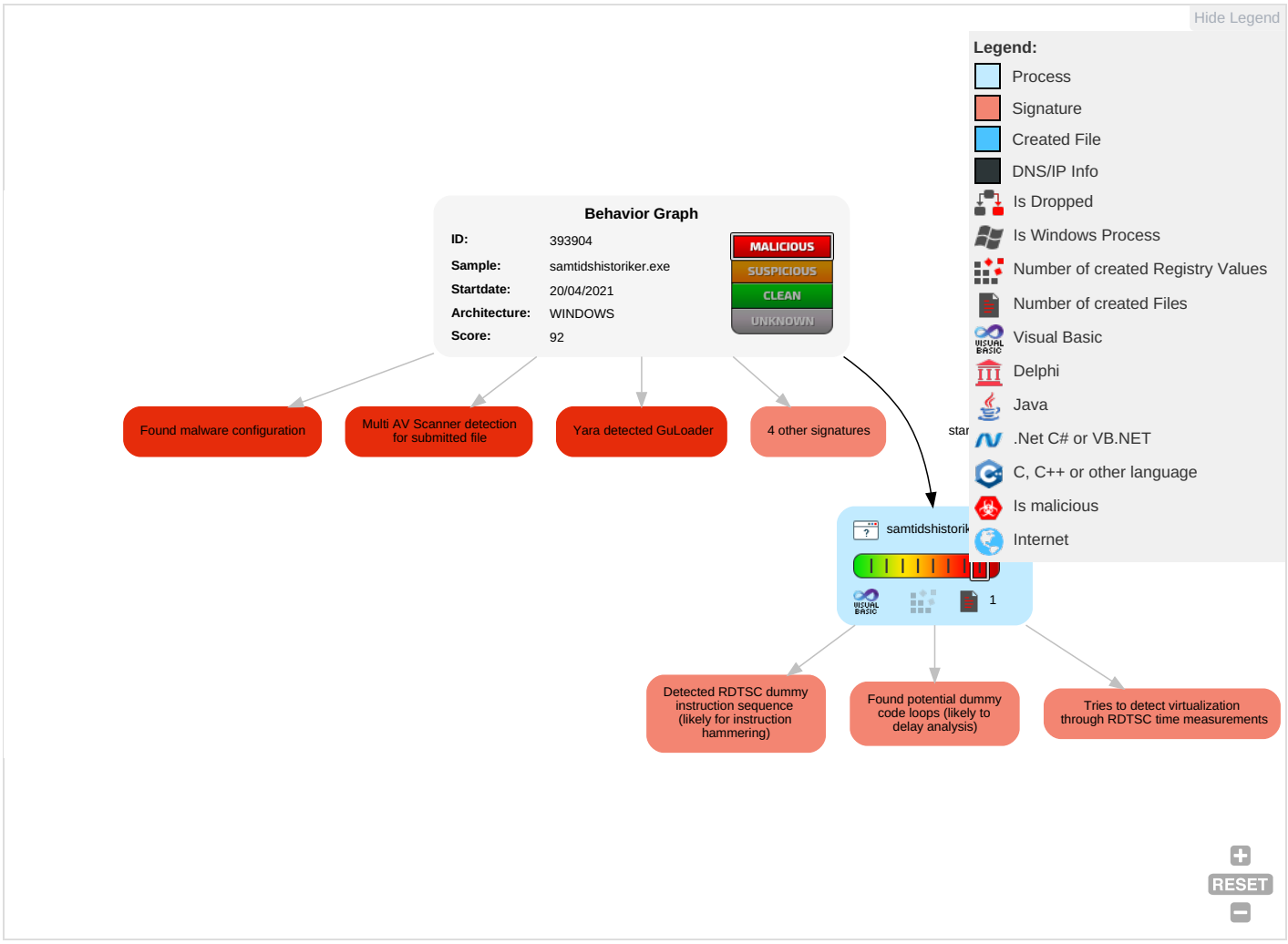
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Virtualization/Sandbox Evasion 1 1	OS Credential Dumping	Security Software Discovery 4 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	O D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	System Information Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	

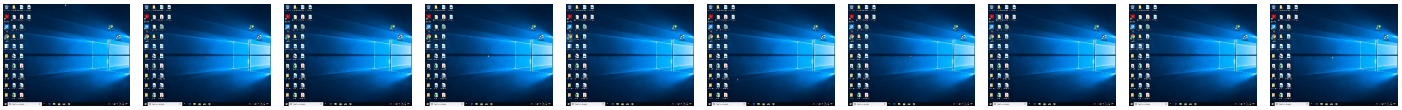
Behavior Graph

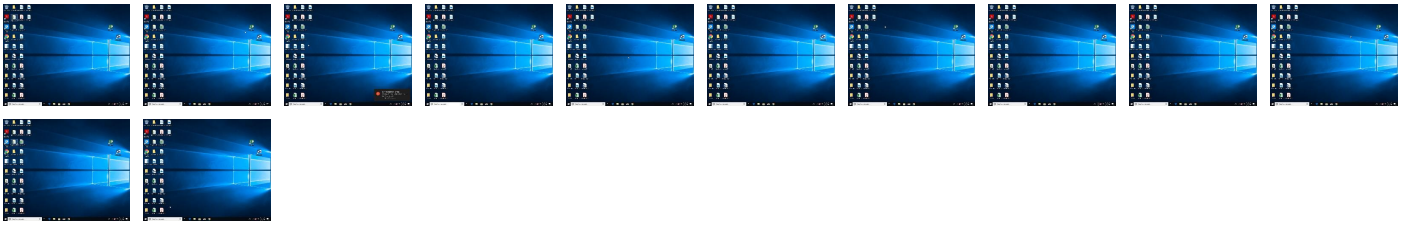


Screenshots

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
samtidshistoriker.exe	24%	Virustotal		Browse
samtidshistoriker.exe	18%	Metadefender		Browse
samtidshistoriker.exe	48%	ReversingLabs	Win32.Worm.Wbvb	
samtidshistoriker.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Copyright Joe Security LLC 2021

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:	31.0.0 Emerald
Analysis ID:	393904
Start date:	20.04.2021
Start time:	21:47:49
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 30s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	samtidshistoriker.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:	14
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:	mal92.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 96.2% (good quality ratio 60.8%) • Quality average: 35% • Quality standard deviation: 32.7%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption

Copyright Joe Security LLC 2021

Warnings:	Show All • Behavior information exceeds normal sizes, reducing to normal. Report will have missing behavior information. • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, backgroundTaskHost.exe, svchost.exe

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):	5.828298088622674
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:	samtidshistoriker.exe
File size:	188416
MD5:	780254149cfe37ce295a82588be31204

General

SHA1:	c28ac373e62a87ae40ad378458d68adc0255558d
SHA256:	74c9a0f54acec0d6579e9a43c75571f05eeb7393f43c13a5e790bfbb262dcb2e
SHA512:	a2808f0288e5405044ed11dd5f61eed846f46309aa891ffc4cc74cc73acd8aef33280459a28225848c317575608d1d680b22dbc0b7818af488390035f02b441b
SSDEEP:	3072:FD6OZu5rkr4/vQkkkkkkkb3KekyOq33poWYgI7xa7gRmwbWV9ECG2Fs8Rmq8NnPa:FW6u5rk8vQkkkkkkkx3pFYlxacUUMOkj
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L...YH.H.....p...p.....#.....@.....

File Icon

Icon Hash:	dadadadaeeced8da

Static PE Info

General

Entrypoint:	0x4023bc
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:	0x48AE4859 [Fri Aug 22 05:02:17 2008 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:	6ffea5264b7d05b326e3dfee0bb6d570

Entrypoint Preview

Instruction
push 00411244h
call 00007F92B4BE3863h
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
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ebx+57CD23B9h], ch
movsd
inc eax
inc esi
lahf
dec edi
sahf
mov bl, 97h
mov al, F8h
jle 00007F92B4BE3872h

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx+66h], al
insb
popad
popad
jnc 00007F92B4BE38E0h
imul ebp, dword ptr [esi+67h], 00736E65h
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or eax, 2EE244E2h
out dx, eax
mov ecx, F08843CDh
rol dword ptr [edx+7C67A070h], FFFFFFFAh
arpl bp, si
daa
in al, C0h
mov ah, 4Bh
wait
or al, A3h
adc byte ptr [ecx+3A467CD2h], al
dec edi
lodsd
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
add byte ptr [eax], al
aam ECh
add byte ptr [eax], al
popfd
jmp far 4900h : 0F000000h
outsb
je 00007F92B4BE38DBh
imul sp, word ptr [ebx+65h], 6572h
xor eax, dword ptr fs:[eax]
or eax, 00000A01h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x27724	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2a000	0x48be	.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	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1a0	.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	0x26d30	0x27000	False	0.367225060096	data	6.06817311982	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x28000	0x1210	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2a000	0x48be	0x5000	False	0.235498046875	data	4.83220983666	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2e456	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x2dace	0x988	data		
RT_ICON	0x2ca26	0x10a8	data		
RT_ICON	0x2a47e	0x25a8	data		
RT_GROUP_ICON	0x2a440	0x3e	data		
RT_VERSION	0x2a180	0x2c0	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, __vbaI2I4, DllFunctionCall, _adj_fpatan, __vbaRedim, __vbaRecUniToAnsi, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaFileOpen, __vbaNew2, __vbaVar2Vec, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarAdd, __vbaVarDup, __vbaStrToAnsi, __vbaFpI4, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	samtidshistoriker
FileVersion	1.00
CompanyName	AbnormalTerm
Comments	AbnormalTerm
ProductName	AbnormalTerm
ProductVersion	1.00
FileDescription	AbnormalTerm
OriginalFilename	samtidshistoriker.exe

Possible Origin

Copyright Joe Security LLC 2021

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: samtidshistoriker.exe PID: 5740 Parent PID: 5692

General

Start time:	21:48:35
Start date:	20/04/2021
Path:	C:\Users\user\Desktop\samtidshistoriker.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\samtidshistoriker.exe'
Imagebase:	0x400000
File size:	188416 bytes
MD5 hash:	780254149CFE37CE295A82588BE31204
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000000.00000002.742722854.0000000000500000.00000040.00000001.sdmp, Author: Joe Security
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