ID: 357302
Sample Name:
EDITORIALIST.exe
Cookbook: default.jbs
Time: 12:31:12
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

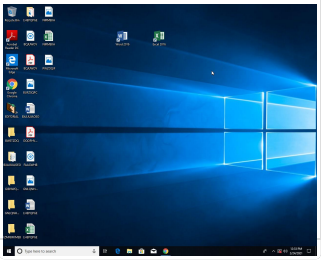
Analysis Report EDITORIALIST.exe

Overview

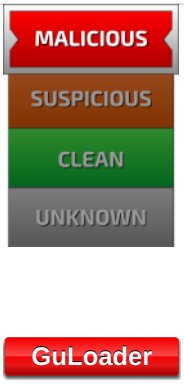
General Information

Sample Name:	EDITORIALIST.exe
Analysis ID:	357302
MD5:	ea23d3d88f6e608.
SHA1:	27e0de4101e73e..
SHA256:	9ac2741f888eeff…
Infos:	

Most interesting Screenshot:



Detection

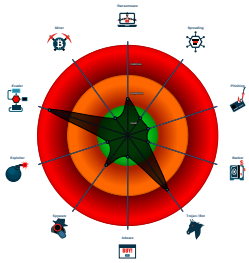


Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Found evasive API chain (may stop…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Writes to foreign memory regions
- Checks if the current process is bein…
- Contains functionality for execution …

Classification



Startup

- **System is w10x64**
- EDITORIALIST.exe (PID: 6844 cmdline: 'C:\Users\user\Desktop\EDITORIALIST.exe' MD5: EA23D3D88F6E6084D4F52D02D261323C)
  - RegAsm.exe (PID: 3480 cmdline: 'C:\Users\user\Desktop\EDITORIALIST.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 6632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

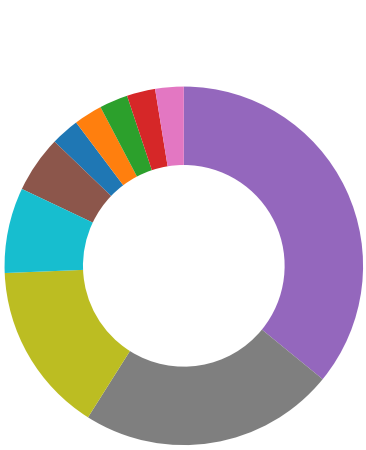
Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.901451594.00000000013C0000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 3480	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Tries to detect Any.run

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:

Contains functionality to hide a thread from the debugger

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

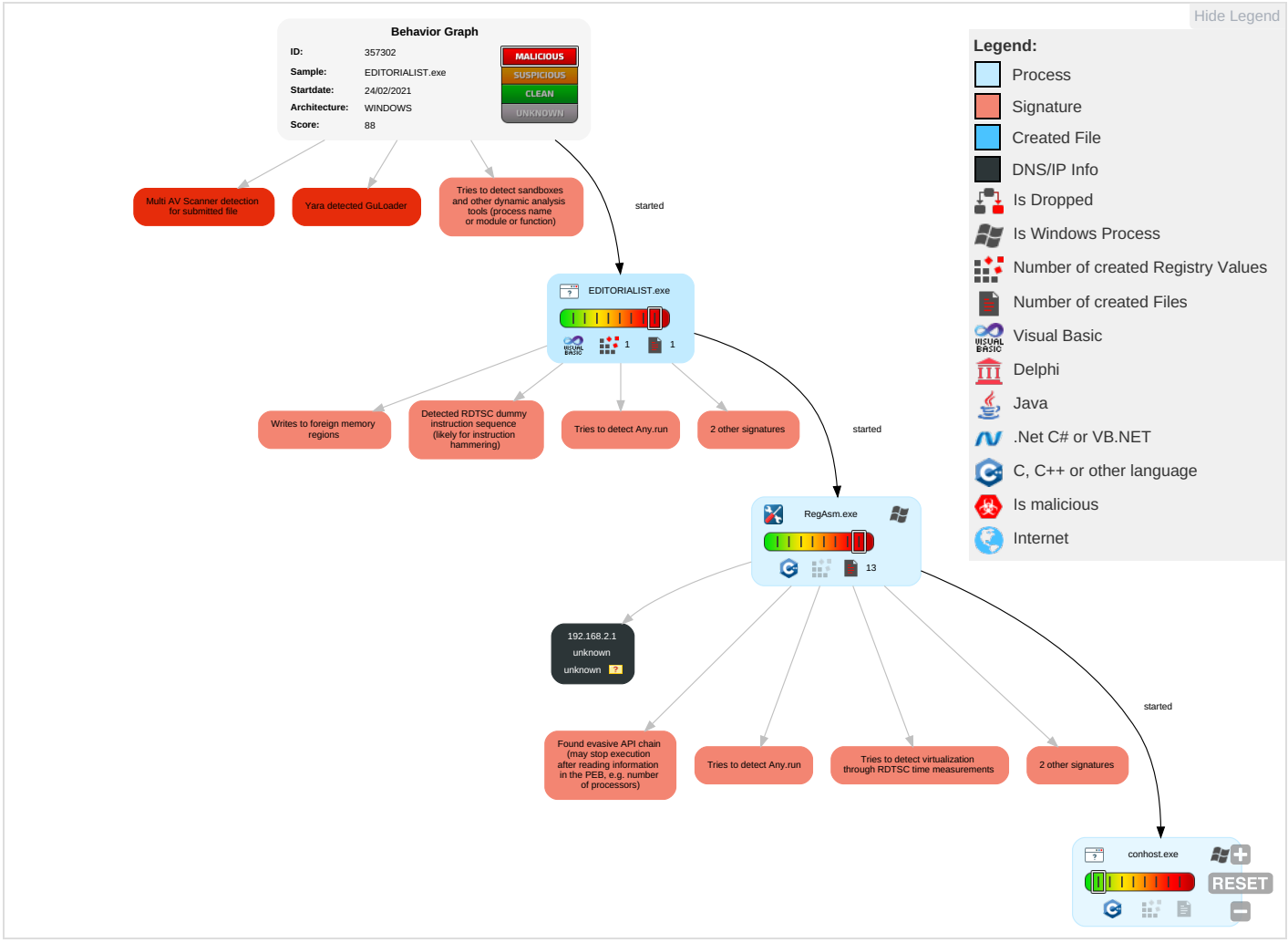
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	F S E
Valid Accounts	Native API 1	DLL Side-Loading 1	Process Injection 1 1 2	Virtualization/Sandbox Evasion 2 2	Input Capture 1	Security Software Discovery 6 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T V A

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	R S E
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 1 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	R V V A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	DLL Side-Loading 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	C D C B
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1	NTDS	System Information Discovery 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

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
EDITORIALIST.exe	64%	Virustotal		Browse
EDITORIALIST.exe	22%	Metadefender		Browse
EDITORIALIST.exe	54%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

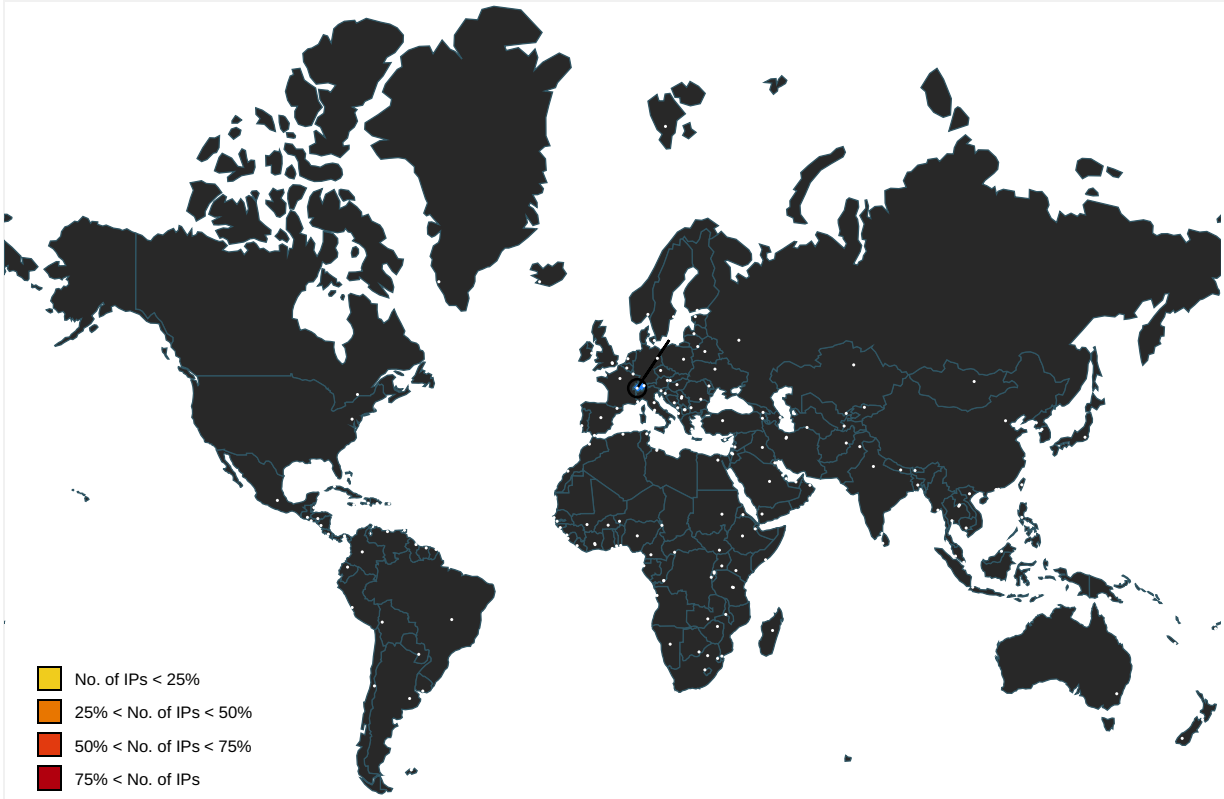
No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357302
Start date:	24.02.2021
Start time:	12:31:12
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EDITORIALIST.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:	15
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:	mal88.troj.evad.winEXE@4/0@0/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 25.9% (good quality ratio 8.6%) • Quality average: 21% • Quality standard deviation: 28.4%
HCA Information:	• Successful, ratio: 72% • 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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 168.61.161.212, 52.255.188.83, 104.43.193.48, 51.11.168.160, 52.155.217.156, 142.250.74.206, 20.54.26.129, 93.184.221.240, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, a1449.dscg2.akamai.net, arc.msn.com, wu.azureedge.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, audownload.windowsupdate.nsatc.net, cs11.wpc.v0cdn.net, hlb.apr-52dd2-0.edgecastdns.net, drive.google.com, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, wu.wpc.apr-52dd2.edgecastdns.net, au-bg-shim.trafficmanager.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, wu.ec.azureedge.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, ctldl.windowsupdate.com, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:32:39	API Interceptor	234x Sleep call for process: RegAsm.exe modified

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):	5.491215363505321
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:	EDITORIALIST.exe
File size:	73728
MD5:	ea23d3d88f6e6084d4f52d02d261323c
SHA1:	27e0de4101e73e0df337c6dc0311d959dbf52416
SHA256:	9ac2741f888eefffdc8085798f5e381536f67dcebfbf5dac2e9e5bf580c03f9a
SHA512:	4e1093446b70e90ad996f670dcdfc1c290a4918ce0078018f43a54ae7d758b52256d74b79afcc3e4350758fb9d37ef34bdf95acbc9d9c43fa8c7b79e6a8cac10
SSDEEP:	1536:LlDDBbvO0nX3NKan/Pn+wB/7sUZ6nYxVSJwD:LlRbvP4a/Pn+wB/7sE6n0ww
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....O.....D.....=.....Rich.....PE..L.....I.....0.....@.....

File Icon

Icon Hash:	1e74f2ea62e4a082

Static PE Info

General

Entrypoint:	0x401494
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:	0x49F80296 [Wed Apr 29 07:32:38 2009 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:	b84199caadebcbcd5f63d7b7de7ff518

Entrypoint Preview

Instruction
push 0040A02Ch
call 00007FBB34A59F43h
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
dec eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ebx+eax*8-49h], dh
jnle 00007FBB34A59EFEh
jnc 00007FBB34A59F12h
dec edx
sahf
aaa
mov eax, dword ptr [2AE23EC9h]
aaa
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
inc ecx
add byte ptr [esi], al
push eax
xchg eax, ebx
add dl, byte ptr [edx+61h]
imul ebp, dword ptr fs:[edi+61h], 7669746Bh
imul esi, dword ptr [ebp+74h], 00003973h
add byte ptr [eax], al
mov byte ptr [ecx+000002F5h], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
or dword ptr [edi], esi
aaa
mov bl, 8Fh
xlatb
bound esp, dword ptr [ebx+5FD6B04Dh]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xf0a4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x12000	0xc14	.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	0x150	.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	0xe644	0xf000	False	0.395735677083	data	6.0319053756	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x10000	0x1218	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x12000	0xc14	0x1000	False	0.265625	data	2.90807398724	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1236c	0x8a8	data		
RT_GROUP_ICON	0x12358	0x14	data		
RT_VERSION	0x120f0	0x268	MS Windows COFF Motorola 68000 object file	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaLenBstr, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, __vbaVarTstEq, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaLateMemCall, __vbaStrToAnsi, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, __vbaVarForNext, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	EDITORIALIST
FileVersion	1.00
CompanyName	Log
ProductName	Log Inverter
ProductVersion	1.00
FileDescription	Log Inverter
OriginalFilename	EDITORIALIST.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map

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

Network Behavior

UDP Packets

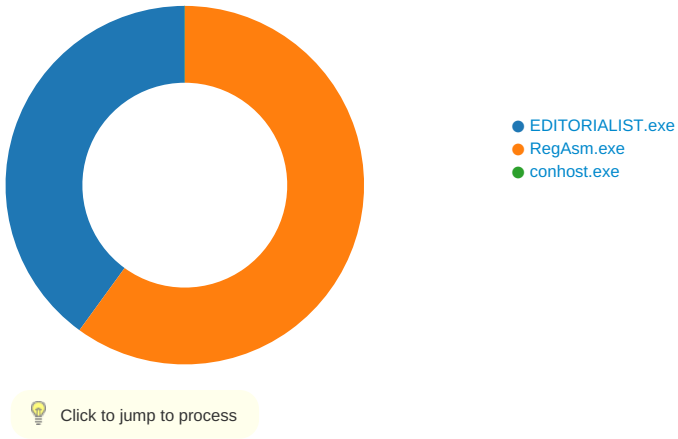
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 12:31:47.708350897 CET	54531	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:31:47.760413885 CET	53	54531	8.8.8.8	192.168.2.4
Feb 24, 2021 12:31:52.282634974 CET	49714	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:31:52.331716061 CET	53	49714	8.8.8.8	192.168.2.4
Feb 24, 2021 12:31:53.790827036 CET	58028	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:31:53.840087891 CET	53	58028	8.8.8.8	192.168.2.4
Feb 24, 2021 12:31:55.388139963 CET	53097	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:31:55.440083027 CET	53	53097	8.8.8.8	192.168.2.4
Feb 24, 2021 12:31:56.313851118 CET	49257	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:31:56.362849951 CET	53	49257	8.8.8.8	192.168.2.4
Feb 24, 2021 12:31:57.085041046 CET	62389	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:31:57.136831045 CET	53	62389	8.8.8.8	192.168.2.4
Feb 24, 2021 12:31:58.418967962 CET	49910	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:31:58.469599009 CET	53	49910	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:00.122687101 CET	55854	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:00.174709082 CET	53	55854	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:01.283230066 CET	64549	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:01.335375071 CET	53	64549	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:05.093066931 CET	63153	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:05.142034054 CET	53	63153	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:06.300709009 CET	52991	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:06.349524975 CET	53	52991	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:07.340379953 CET	53700	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:07.392235994 CET	53	53700	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:08.281455994 CET	51726	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:08.346898079 CET	53	51726	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:12.288232088 CET	56794	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:12.350832939 CET	53	56794	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:14.024910927 CET	56534	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:14.073790073 CET	53	56534	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:15.024653912 CET	56627	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:15.076423883 CET	53	56627	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:15.885713100 CET	56621	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:15.934597969 CET	53	56621	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:17.145350933 CET	63116	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:17.194421053 CET	53	63116	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:20.857116938 CET	64078	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:20.909058094 CET	53	64078	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:37.891499996 CET	64801	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:37.949184895 CET	53	64801	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:38.987286091 CET	61721	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:39.051724911 CET	53	61721	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:39.538017988 CET	51255	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:39.608546972 CET	53	51255	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:39.668736935 CET	61522	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:39.730603933 CET	53	61522	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:40.193236113 CET	52337	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:40.258877039 CET	53	52337	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 12:32:40.748047113 CET	55046	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:40.810791969 CET	53	55046	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:40.888029099 CET	49612	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:40.967439890 CET	53	49612	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:41.350810051 CET	49285	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:41.413418055 CET	53	49285	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:42.080142021 CET	50601	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:42.129075050 CET	53	50601	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:42.844948053 CET	60875	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:42.852648973 CET	56448	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:42.893976927 CET	53	60875	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:42.901678085 CET	53	56448	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:43.832237005 CET	59172	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:43.881315947 CET	53	59172	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:44.319447041 CET	62420	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:44.369136095 CET	53	62420	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:56.550116062 CET	60579	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:56.599226952 CET	53	60579	8.8.8.8	192.168.2.4
Feb 24, 2021 12:32:56.608593941 CET	50183	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:32:56.680665016 CET	53	50183	8.8.8.8	192.168.2.4
Feb 24, 2021 12:33:01.436084986 CET	61531	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:33:01.494746923 CET	53	61531	8.8.8.8	192.168.2.4
Feb 24, 2021 12:33:31.898732901 CET	49228	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:33:31.948085070 CET	53	49228	8.8.8.8	192.168.2.4
Feb 24, 2021 12:33:33.869833946 CET	59794	53	192.168.2.4	8.8.8.8
Feb 24, 2021 12:33:33.936659098 CET	53	59794	8.8.8.8	192.168.2.4

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EDITORIALIST.exe PID: 6844 Parent PID: 5996

General

Start time:	12:31:54
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\EDITORIALIST.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\EDITORIALIST.exe'
Imagebase:	0x400000
File size:	73728 bytes
MD5 hash:	EA23D3D88F6E6084D4F52D02D261323C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING	success or wait	1	660E2872	RegCreateKeyW
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING\Sequences	success or wait	1	660E2872	RegCreateKeyW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\VB and VBA Program Settings\TANKRENSNING\Sequences	Koinciderede4	unicode	MS Sans Serif	success or wait	1	660E2183	RegSetValueExW

Analysis Process: RegAsm.exe PID: 3480 Parent PID: 6844

General

Start time:	12:32:21
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\EDITORIALIST.exe'
Imagebase:	0xfe0000
File size:	64616 bytes
MD5 hash:	6FD7592411112729BF6B1F2F6C34899F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000003.00000002.901451594.00000000013C0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13C2E27	InternetOpenUrlA
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	13C2E27	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13C2E27	InternetOpenUrlA
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	13C2E27	InternetOpenUrlA
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	13C2E27	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	13C2E27	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6632 Parent PID: 3480

General

Start time:	12:32:21
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis