ID: 357559
Sample Name:
LIZvq3EW7m.exe
Cookbook: default.jbs
Time: 18:35:39
Date: 24/02/2021
Version: 31.0.0 Emerald

Table of Contents

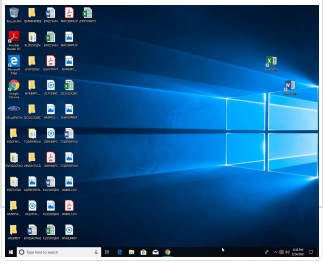
Analysis Report LIZvq3EW7m.exe

Overview

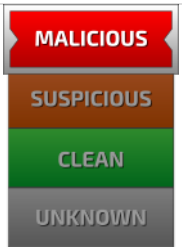
General Information

Sample Name:	LIZvq3EW7m.exe
Analysis ID:	357559
MD5:	5d2d34449323c6..
SHA1:	a48c7f51db44ca8..
SHA256:	95a1ff3f5d08ac3…
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



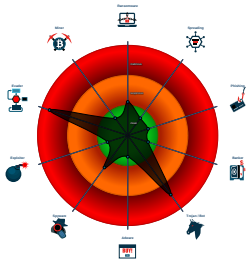
AgentTesla GuLoader

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected GuLoader
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Writes to foreign memory regions
- Abnormal high CPU Usage

Classification



Startup

- **System is w10x64**
- LIZvq3EW7m.exe (PID: 6288 cmdline: 'C:\Users\user\Desktop\LIZvq3EW7m.exe' MD5: 5D2D34449323C67BA1F5EC7561DF2204)
  - RegAsm.exe (PID: 6728 cmdline: 'C:\Users\user\Desktop\LIZvq3EW7m.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - conhost.exe (PID: 4632 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

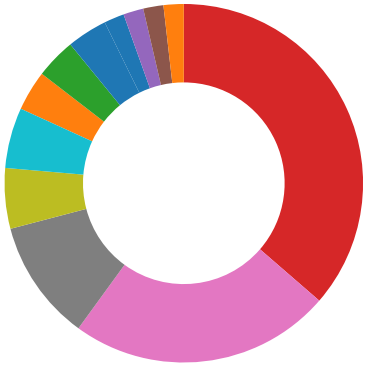
Source	Rule	Description	Author	Strings
0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0000000E.00000002.510534238.0000000000B42000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6728	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Process Memory Space: RegAsm.exe PID: 6728	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Click to see the 1 entries

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
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

Uses new MSVCR Dlls

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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:

Hides threads from debuggers

HIPS / PFW / Operating System Protection Evasion:

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected AgentTesla

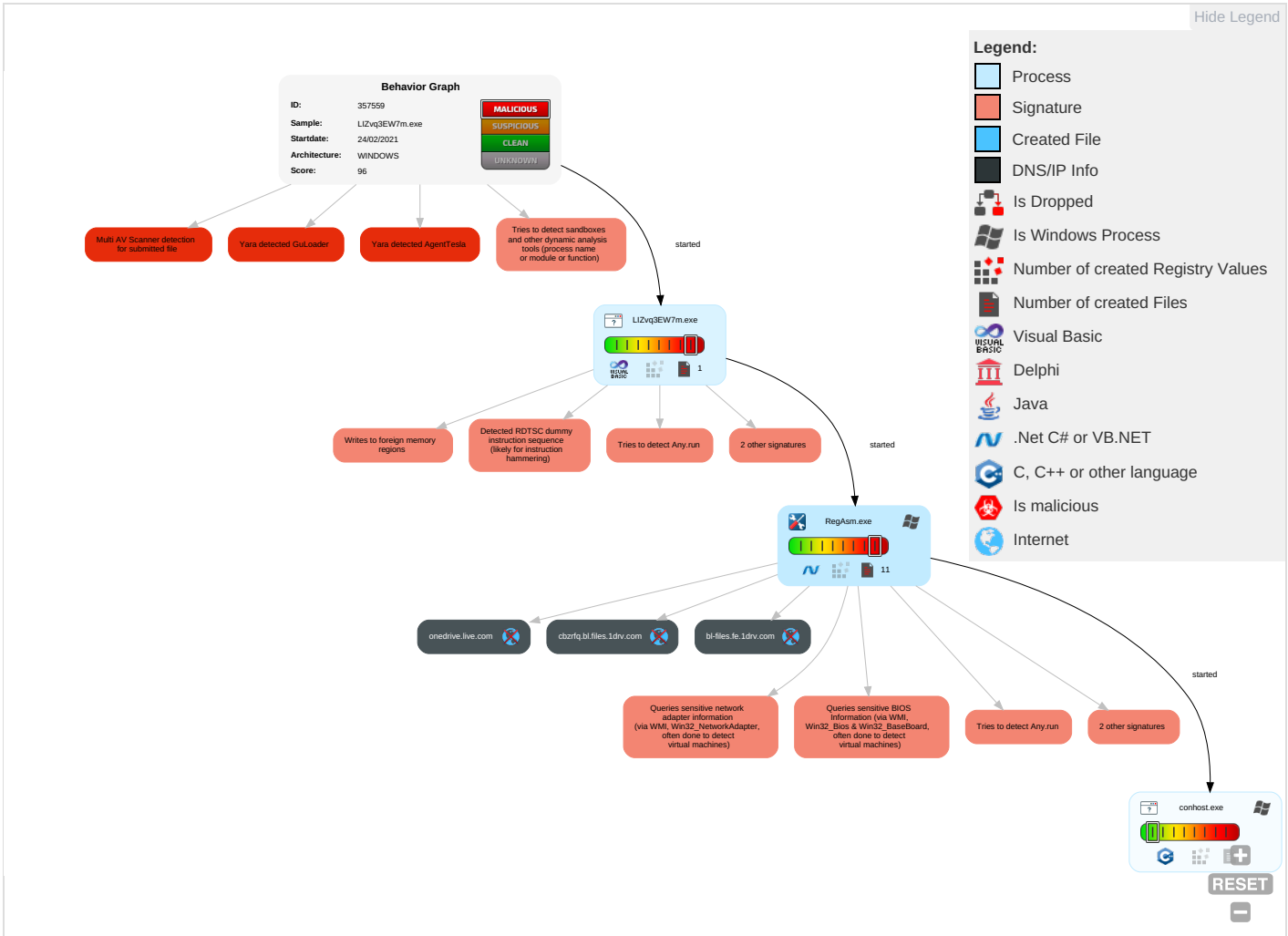
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Net Effe
Valid Accounts	Windows Management Instrumentation 2 1 1	DLL Side-Loading 1	Access Token Manipulation 1	Virtualization/Sandbox Evasion 3 4	OS Credential Dumping	Security Software Discovery 6 3 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Non-Application Layer Protocol 1	Eav Inse Net Cor
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Process Injection 1 1 2	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 3 4	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exp Rec Cal
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Access Token Manipulation 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exp Tra Loc
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	System Information Discovery 3 2 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Swa
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mai Dev Cor

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
LIZvq3EW7m.exe	21%	Virustotal		Browse
LIZvq3EW7m.exe	17%	ReversingLabs	Win32.Trojan.Razy	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://JSQBKI.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
onedrive.live.com	unknown	unknown	false		high
cbzrfq.bl.files.1drv.com	unknown	unknown	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://onedrive.live.com/B	RegAsm.exe, 0000000E.00000002.510872582.0000000000F1B000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/R	RegAsm.exe, 0000000E.00000002.510872582.0000000000F1B000.00000004.00000020.sdmp	false		high
http://127.0.0.1:HTTP/1.1	RegAsm.exe, 0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://api.ipify.org%GETMozilla/5.0	RegAsm.exe, 0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://DynDns.comDynDNS	RegAsm.exe, 0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cbzrfq.bl.files.1drv.com/t	RegAsm.exe, 0000000E.00000002.510872582.0000000000F1B000.00000004.00000020.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	RegAsm.exe, 0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://JSQBKI.com	RegAsm.exe, 0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cbzrfq.bl.files.1drv.com/y4m6xg1XvMW3gbVxDaG8eC-sQOlr6nmG4uqhmYHacvOjJxUricSauwypPs7Fa6xUXOy	RegAsm.exe, 0000000E.00000002.510872582.0000000000F1B000.00000004.00000020.sdmp	false		high
http://https://onedrive.live.com/download?cid=F57CEB019EB26E7D&resid=F57CEB019EB26E7D%21108&authkey=AN1oxHG	RegAsm.exe	false		high
http://https://cbzrfq.bl.files.1drv.com/X	RegAsm.exe, 0000000E.00000002.510872582.0000000000F1B000.00000004.00000020.sdmp	false		high
http://https://cbzrfq.bl.files.1drv.com/y4meC4ccKelBPgeKSh6hZT6bRCOR5ff4nvnt28NLuAcRP3PcWBKUwkBGKN3LJUa7F0I	RegAsm.exe, 0000000E.00000002.510930369.0000000000F5E000.00000004.00000020.sdmp	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	357559
Start date:	24.02.2021
Start time:	18:35:39
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LIZvq3EW7m.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:	23
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:	mal96.troj.evad.winEXE@4/0@2/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 90% • 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): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, WmiPrvSE.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 104.42.151.234, 13.64.90.137, 168.61.161.212, 184.30.24.56, 52.255.188.83, 23.211.6.115, 51.104.146.109, 51.103.5.186, 92.122.213.194, 92.122.213.247, 51.104.139.180, 13.107.42.13, 13.107.42.12, 20.54.26.129 • Excluded domains from analysis (whitelisted): odc-web-brs.onedrive.akadns.net, arc.msn.com.nsatc.net, store-images.s-microsoft.com-c.edgekey.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, l-0004.l-msedge.net, e12564.dspb.akamaiedge.net, wns.notify.trafficmanager.net, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, l-0003.l-msedge.net, odc-bl-files-brs.onedrive.akadns.net, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, odc-bl-files-geo.onedrive.akadns.net, skypedataprdcolwus17.cloudapp.net, client.wns.windows.com, fs.microsoft.com, odc-web-geo.onedrive.akadns.net, bl-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, ris-prod.trafficmanager.net, skypedataprdcolcus17.cloudapp.net, e1723.g.akamaiedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net, vip2-par02p.wns.notify.trafficmanager.net • 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 NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:38:20	API Interceptor	199x 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):	4.79650156443488
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:	LIZvq3EW7m.exe
File size:	131072
MD5:	5d2d34449323c67ba1f5ec7561df2204
SHA1:	a48c7f51db44ca8a2b0240d9c57c1983ac5d75dd
SHA256:	95a1ff3f5d08ac3d0dfe64300eec668fa0c78bdb7da395f1d91735c5a0aef8a5
SHA512:	28b4c6df609084045f866686e559c7771b6455bc8fde56942f9422265c6ed2acfe12ef383c23225ad171d9d7ba22efc9ef7137c069070812af798edaa8ae6d73
SSDEEP:	1536:HWWTwV4fVhuy/kysvxhG7NuX40vbyovaWm5vj2kht/uxVQwV4MjW:7wVUPsyChtX40Tyova75vj2mt/QqwV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....u...1...1...1.....0...~...0.....0...Rich1.....PE..L...n\RK.....P.....`....@.....

File Icon

Icon Hash:	01d292796dda0080

Static PE Info

General

Entrypoint:	0x4013dc
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:	0x4B525C6E [Sun Jan 17 00:40:14 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4

General

OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	cc882d101998a701353b40b0cd8c341a

Entrypoint Preview

Instruction
push 00412024h
call 00007FE178CB4923h
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 cl, bl
dec esi
aad 21h
nop
pop ebp
inc ebp
inc ecx
sub byte ptr [ebx+76h], FFFFFF80h
mov edi, 0045384Ch
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+eax], al
add byte ptr [eax], al
inc edx
inc ebp
dec esi
inc edi
dec esp
inc ebp
push edx
push ebx
add byte ptr [eax+00000059h], ah
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
add al, 32h
int 5Ah
je 00007FE178CB48D5h
sbb eax, dword ptr [edi+41h]
mov eax, 337E19C3h
mov dword ptr [D3AAF464h], eax
pop ebp
nop
outsb
out dx, al
aad 47h
mov ah, 46h
sub dword ptr [eax+5Eh], 3A62DA2Dh

Instruction
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
inc ebp
or eax, dword ptr [ecx]
add byte ptr [edx+0000007Fh], bl
sldt word ptr [esi+79h]
jc 00007FE178CB499Bh
outsb
jnc 00007FE178CB49A6h
jnc 00007FE178CB49A1h
outsb
outsb
jnc 00007FE178CB4965h
add byte ptr [00000601h], cl

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x15214	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x83ce	.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	0xe0	.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	0x14644	0x15000	False	0.392857142857	data	5.46295201906	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.data	0x16000	0xa18	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x83ce	0x9000	False	0.339952256944	data	3.52770935798	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1f2a6	0x128	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1dc7e	0x1628	dBase IV DBT of \200.DBF, blocks size 0, block length 4608, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1bfd6	0x1ca8	data		
RT_ICON	0x1b32e	0xca8	data		
RT_ICON	0x1afc6	0x368	GLS_BINARY_LSB_FIRST		
RT_ICON	0x18a1e	0x25a8	data		
RT_ICON	0x17976	0x10a8	data		
RT_ICON	0x1750e	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x17498	0x76	data		
RT_VERSION	0x17240	0x258	data		

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaLateMemCall, __vbaVarDup, _CIatan, __vbaStrMove, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0000 0x04b0
InternalName	udfrlig
FileVersion	1.00
CompanyName	Sinth Radio
ProductName	Sinth Radio
ProductVersion	1.00
FileDescription	Sinth Radio
OriginalFilename	udfrlig.exe

Network Behavior

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 18:36:32.208460093 CET	49557	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:32.257194042 CET	53	49557	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:33.422243118 CET	61733	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:33.472306967 CET	53	61733	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:34.592509985 CET	65447	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:34.641379118 CET	53	65447	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:43.666870117 CET	52441	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:43.720164061 CET	53	52441	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:47.061758041 CET	62176	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:47.112010956 CET	53	62176	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:48.366338015 CET	59596	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:48.416636944 CET	53	59596	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:48.720249891 CET	65296	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:48.783117056 CET	53	65296	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:49.668557882 CET	63183	53	192.168.2.5	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 24, 2021 18:36:49.720951080 CET	53	63183	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:50.927479982 CET	60151	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:50.976226091 CET	53	60151	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:51.810408115 CET	56969	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:51.867913961 CET	53	56969	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:52.765450001 CET	55161	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:52.814199924 CET	53	55161	8.8.8.8	192.168.2.5
Feb 24, 2021 18:36:53.611812115 CET	54757	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:36:53.670384884 CET	53	54757	8.8.8.8	192.168.2.5
Feb 24, 2021 18:37:07.737047911 CET	49992	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:37:07.785698891 CET	53	49992	8.8.8.8	192.168.2.5
Feb 24, 2021 18:37:30.320733070 CET	60075	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:37:30.379899979 CET	53	60075	8.8.8.8	192.168.2.5
Feb 24, 2021 18:37:37.036969900 CET	55016	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:37:37.095369101 CET	53	55016	8.8.8.8	192.168.2.5
Feb 24, 2021 18:38:08.992552996 CET	64345	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:38:09.044436932 CET	53	64345	8.8.8.8	192.168.2.5
Feb 24, 2021 18:38:11.223117113 CET	57128	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:38:11.272001982 CET	53	57128	8.8.8.8	192.168.2.5
Feb 24, 2021 18:38:11.842854023 CET	54791	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:38:11.947535992 CET	53	54791	8.8.8.8	192.168.2.5
Feb 24, 2021 18:38:26.526025057 CET	50463	53	192.168.2.5	8.8.8.8
Feb 24, 2021 18:38:26.588095903 CET	53	50463	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 24, 2021 18:38:11.223117113 CET	192.168.2.5	8.8.8.8	0xca67	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)
Feb 24, 2021 18:38:11.842854023 CET	192.168.2.5	8.8.8.8	0x1e7c	Standard query (0)	cbzrfq.bl.files.1drv.com	A (IP address)	IN (0x0001)

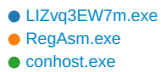
DNS Answers

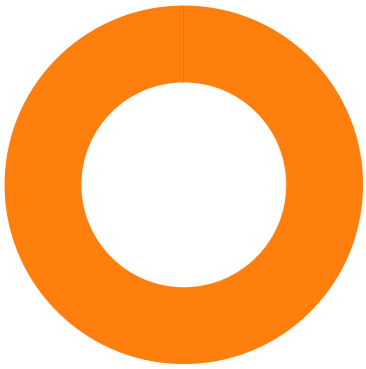
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 24, 2021 18:38:11.272001982 CET	8.8.8.8	192.168.2.5	0xca67	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 18:38:11.947535992 CET	8.8.8.8	192.168.2.5	0x1e7c	No error (0)	cbzrfq.bl.files.1drv.com	bl-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)
Feb 24, 2021 18:38:11.947535992 CET	8.8.8.8	192.168.2.5	0x1e7c	No error (0)	bl-files.fe.1drv.com	odc-bl-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior





Click to jump to process

System Behavior

Analysis Process: LIZvq3EW7m.exe PID: 6288 Parent PID: 5756

General

Start time:	18:36:39
Start date:	24/02/2021
Path:	C:\Users\user\Desktop\LIZvq3EW7m.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LIZvq3EW7m.exe'
Imagebase:	0x400000
File size:	131072 bytes
MD5 hash:	5D2D34449323C67BA1F5EC7561DF2204
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

Analysis Process: RegAsm.exe PID: 6728 Parent PID: 6288

General

Start time:	18:38:00
Start date:	24/02/2021
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\LIZvq3EW7m.exe'
Imagebase:	0x770000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.515531566.000000001D861000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 0000000E.00000002.510534238.0000000000B42000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

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	B44400	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	B44400	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	B44400	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	B44400	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	B44400	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	B44400	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	732260AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	732260AC	unknown
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	732260AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	732260AC	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73255544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73255544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73255544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73255544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	73258738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	73258738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73258738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73255544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	73255544	unknown

Analysis Process: conhost.exe PID: 4632 Parent PID: 6728

General

Start time:	18:38:00
Start date:	24/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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