ID: 830606
Sample Name: Solicitud de presupuesto.exe
Cookbook: default.jbs
Time: 14:34:20
Date: 20/03/2023
Version: 37.0.0 Beryl

Table of Contents

Table of Contents 2
Windows Analysis Report Solicitud de presupuesto.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Threat Intel 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Signatures 5
Memory Dumps 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 5
AV Detection 5
Networking 5
System Summary 5
Data Obfuscation 5
Malware Analysis System Evasion 6
Anti Debugging 6
Stealing of Sensitive Information 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 9
URLs from Memory and Binaries 9
World Map of Contacted IPs 9
Public IPs 9
General Information 10
Warnings 10
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASNs 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 11
General 11
File Icon 11
Static PE Info 11
General 11
Entrypoint Preview 12
Data Directories 12
Sections 13
Resources 13
Imports 13
Possible Origin 13
Network Behavior 13
Network Port Distribution 13
TCP Packets 14
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
Statistics 16
Behavior 16
System Behavior 16

Analysis Process: Solicitud de presupuesto.exePID: 5800, Parent PID: 3324 16
General 16
File Activities 17
Analysis Process: Solicitud de presupuesto.exePID: 1352, Parent PID: 5800 17
General 17
File Activities 17
File Created 17
Disassembly 18

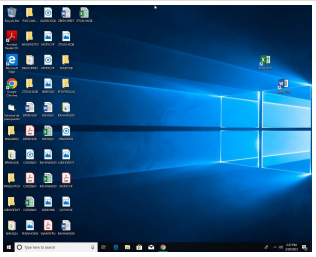
Windows Analysis Report

Solicitud de presupuesto.exe

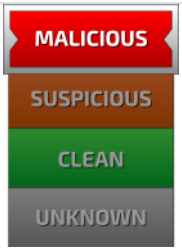
Overview

General Information

Sample Name:	Solicitud de presupuesto.exe
Analysis ID:	830606
MD5:	e6f54ce2be485..
SHA1:	f609993ae9cac..
SHA256:	69e3a2462654...
Infos:	



Detection



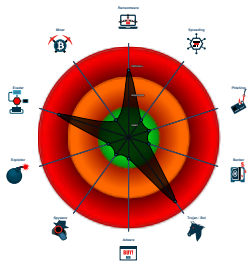
GuLoader

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

Signatures

- Antivirus / Scanner detection for sub…
- Potential malicious icon found
- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- GuLoader behavior detected
- Yara detected GuLoader
- Hides threads from debuggers
- Tries to detect virtualization through…
- Contains functionality to hide a threa…
- C2 URLs / IPs found in malware con…
- Yara detected VB6 Downloader Gen…
- Machine Learning detection for sam…

Classification



Process Tree

- **System is w10x64**
- Solicitud de presupuesto.exe (PID: 5800 cmdline: C:\Users\user\Desktop\Solicitud de presupuesto.exe MD5: E6F54CE2BE4854FDCA9C97450C347A2C)
  - Solicitud de presupuesto.exe (PID: 1352 cmdline: C:\Users\user\Desktop\Solicitud de presupuesto.exe MD5: E6F54CE2BE4854FDCA9C97450C347A2C)
- **cleanup**

Malware Threat Intel

Provided by malpedia

Name	Description	Attribution	Blogpost URLs	Link
CloudEyE, GuLoader	CloudEyE (initially named GuLoader) is a small VB5/6 downloader. It typically downloads RATs/Stealers, such as Agent Tesla, Arkei/Vidar, Formbook, Lokibot, Netwire and Remcos, often but not always from Google Drive. The downloaded payload is xored.	No Attribution	http://https://0x00sec.org/t/analyzing-modern-malware-techniques-part-3/18943https://blog.malwarebytes.com/scams/2020/08/sba-phishing-scams-from-malware-to-advanced-social-engineering/https://blog.morphisec.com/guloader-the-rat-downloaderhttps://blog.vincss.net/2020/05/re014-guloader-antivm-techniques.htmlhttps://cert-agid.gov.it/news/malware/tecniche-per-semplificare-lanalisi-del-malware-guloader/	http://https://malpedia.caad.fkie.fraunhofer.de/details/win.cloudeye

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://www.mediafire.com/file/9yrjccjdow659ow/sala_ziPUQPqut175.bin/file",
  "User Agent": "Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.307522232.000000000040D000.00000020.00000001.01000000.00000003.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth (Nextron Systems)	• 0x1a5c:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000001.00000000.403982899.000000000040D000.00000020.00000001.01000000.00000003.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth (Nextron Systems)	• 0x1a5c:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000000.00000002.404604650.000000000040D000.00000020.00000001.01000000.00000003.sdmp	LokiBot_Dropper_Packed_R11_Feb18	Auto-generated rule - file scan copy.pdf.r11	Florian Roth (Nextron Systems)	• 0x1a5c:$s1: C:\Program Files (x86)\Microsoft Visual Studio\VB98\VB6.OLB
00000001.00000002.575875706.0000000000560000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: Solicitud de presupuesto.exe PID: 1352	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	

Click to see the 1 entries

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking

C2 URLs / IPs found in malware configuration

System Summary

Potential malicious icon found

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion

Tries to detect virtualization through RDTSC time measurements

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Anti Debugging

Hides threads from debuggers

Contains functionality to hide a thread from the debugger

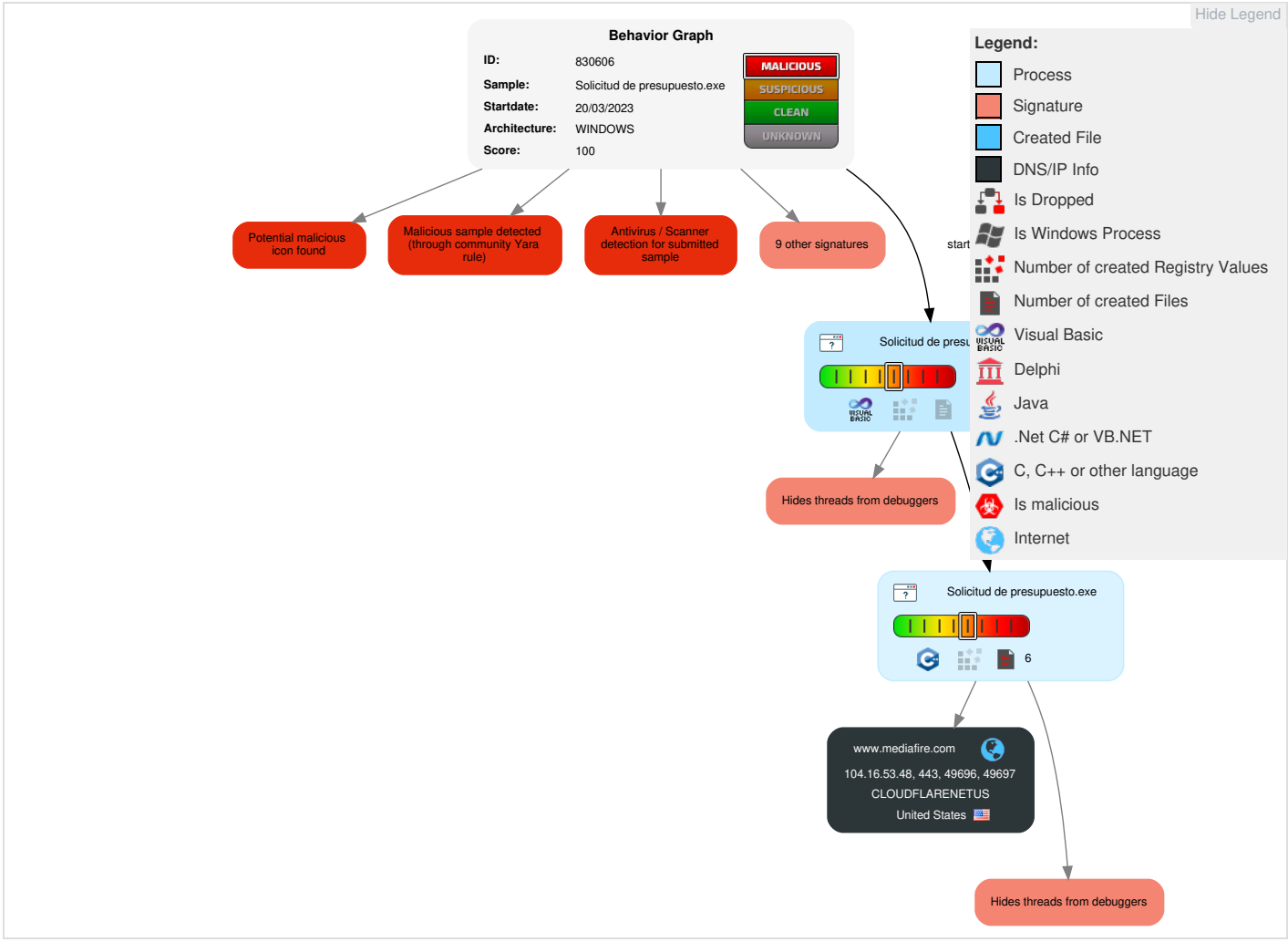
Stealing of Sensitive Information

GuLoader behavior detected

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	1 1 Process Injection	1 2 Virtualization/Sandbox Evasion	OS Credential Dumping	4 2 1 Security Software Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	1 Encrypted Channel	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 Software Packing	LSASS Memory	1 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	2 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 1 Process Injection	Security Account Manager	2 1 System Information Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 1 3 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 Ingress Tool Transfer	SIM Card Swap		Carrier Billing Fraud

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
Solicitud de presupuesto.exe	79%	Virustotal		Browse
Solicitud de presupuesto.exe	71%	ReversingLabs	Win32.Infostealer.Fareit	
Solicitud de presupuesto.exe	100%	Avira	TR/Injector.akytx	
Solicitud de presupuesto.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.Solicitud de presupuesto.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1239136		Download File
1.0.Solicitud de presupuesto.exe.400000.0.unpack	100%	Avira	TR/Injector.akytx		Download File
0.0.Solicitud de presupuesto.exe.400000.0.unpack	100%	Avira	TR/Injector.akytx		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http:// https://static.cloudflareinsights.com/beacon.min.js/vaafb692b2aea4879b33c060e79fe946216663173699 93	0%	URL Reputation	safe	
http:// https://static.cloudflareinsights.com/beacon.min.js/vaafb692b2aea4879b33c060e79fe946216663173699 93	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.mediafire.com	104.16.53.48	true	false		high

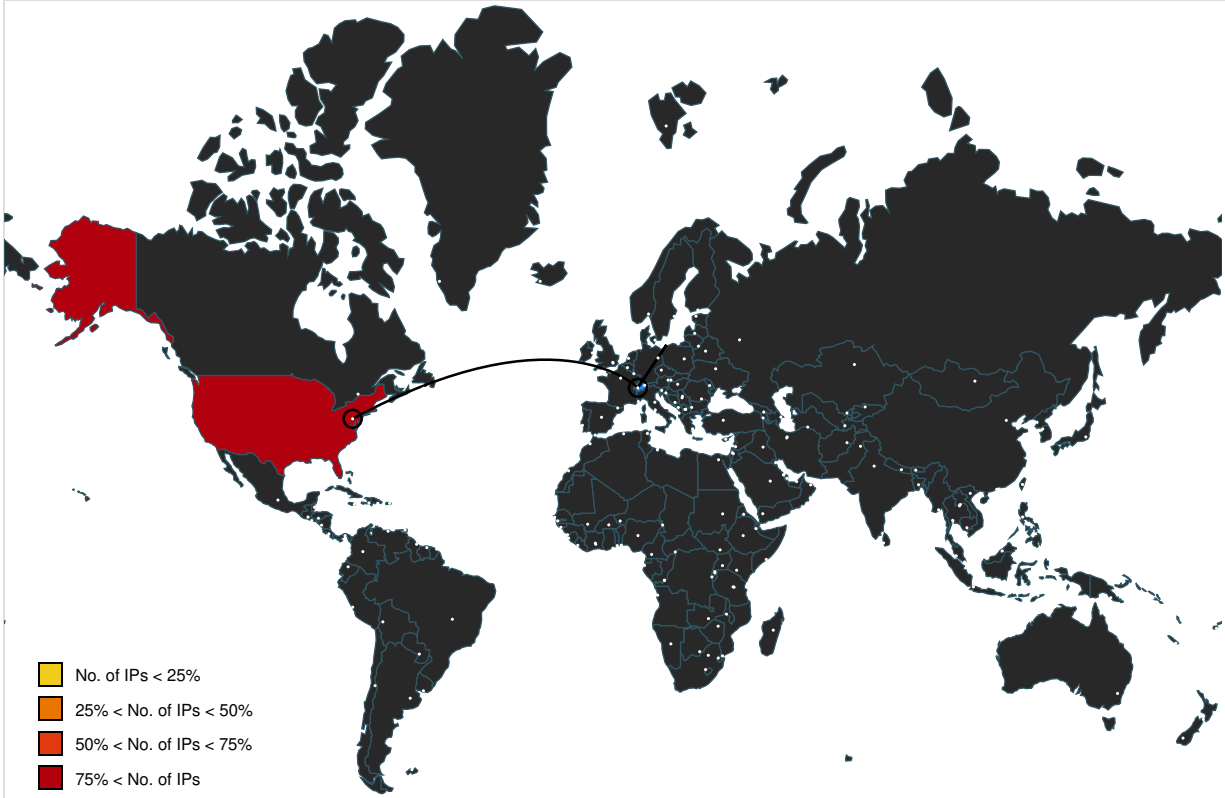
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://www.mediafire.com/error.php?errno=386&quickkey=9yrjccjdow659ow&origin=download	false		high
http://https://www.mediafire.com/file/9yrjccjdow659ow/sala_ziPUQPqut175.bin/file	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https://static.cloudflareinsights.com/beacon.min.js/vaaf b692b2aea4879b33c060e79fe94621666317369993	Solicitud de presupuesto.exe, 00000001.00000002.57 6110769.0000000002380000.00000004.000008 00.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.53.48	www.mediafire.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	37.0.0 Beryl
Analysis ID:	830606
Start date and time:	2023-03-20 14:34:20 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	5
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
Sample file name:	Solicitud de presupuesto.exe
Detection:	MAL
Classification:	mal100.rans.troj.evad.winEXE@3/0@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 93.7% (good quality ratio 78%) • Quality average: 60.8% • Quality standard deviation: 36.1%
HCA Information:	• Successful, ratio: 89% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, WMIADAP.exe, conhost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtDeviceIoControlFile 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
14:36:23	API Interceptor	46x Sleep call for process: Solicitud de presupuesto.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

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	3.4800524608313186
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:	Solicitud de presupuesto.exe
File size:	86016
MD5:	e6f54ce2be4854fdca9c97450c347a2c
SHA1:	f609993ae9cace1abf742553a12a21852d363d5d
SHA256:	69e3a2462654341256f2feb5c86c1c8bb514d9ab97a02917cd22640c1474cac9
SHA512:	ffb515155cf5fc93ee30448f6e015bc734a08b2e088ab5c66cfd1aa2c8becf77ffc070e12d9c7e0de54eefda775e19b650d3fe072a78a0841c498453d85bdb94
SSDEEP:	768:dNMBz7H9ernso9wD9/St9vpQr5WDdgUWih1jwZAvF/fJ8P5MHzZt:cBlernso94SbZdgUWih1j0AvF/B8xkb
TLSH:	5C833816B2C8E831D95206F11E315BA484267C354A049A43F7483F3EBB7FEA7A7A0717
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,..SM..SM..SM...Q..RM...o..UM..ek..RM..RichSM.....PE..L....(.M..... ... .0....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x40148c
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	RELOCS_STRIPPED, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, 32BIT_MACHINE
DLL Characteristics:	
Time Stamp:	0x4D8A28DA [Wed Mar 23 17:07:38 2011 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:	965ac96787cf85955888f8a9a62bd475

Entrypoint Preview

Instruction
push 0040E028h
call 00007FD4ACA97FB5h
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 [esp+ecx*4], ch
mov bl, byte ptr [eax-1Fh]
and eax, 16B745E3h
adc dword ptr [ebp+ebp+0097B581h], edi
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+6Eh], ch
jnc 00007FD4ACA98037h
insb
popad
push 00007265h
adc byte ptr [esi], cl
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax
push es
xchg bh, al
cmp dword ptr [edx+444CE5AAh], FFFFFFB8h
add eax, F269B13Ch
or eax, D270823Ch
jno 00007FD4ACA97FCEh
out E8h, eax
inc edx
pop dword ptr [ebx+68h]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11f54	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x14000	0x8f4	.rsrc

Name	Virtual Address	Virtual Size	Is in Section
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	0x230	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x14c	.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	0x1144c	0x12000	False	0.2748480902777778	data	3.8233408809320486	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x13000	0xc10	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x14000	0x8f4	0x1000	False	0.16943359375	data	1.971156033648951	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x147c4	0x130	Device independent bitmap graphic, 32 x 64 x 1, image size 256		
RT_ICON	0x144dc	0x2e8	Device independent bitmap graphic, 32 x 64 x 4, image size 640		
RT_ICON	0x143b4	0x128	Device independent bitmap graphic, 16 x 32 x 4, image size 192		
RT_GROUP_ICON	0x14384	0x30	data		
RT_VERSION	0x14150	0x234	data	English	United States

Imports

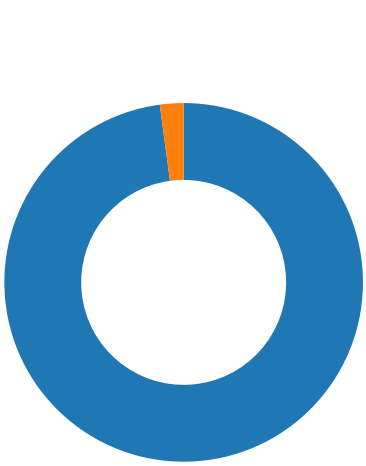
DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaHresultCheck, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, _adj_fprem1, __vbaStrCat, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, _adj_fpatan, EVENT_SINK_Release, __vbaUI1I2, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaI2Str, __vbaFPException, _CIlog, __vbaNew2, __vbaR8Str, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaInStrB, __vbaVarDup, _CIatan, __vbaStrMove, __vbaUI1Str, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Possible Origin

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

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 14:36:22.177046061 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:22.177133083 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:22.177280903 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:22.194329977 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:22.194384098 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:22.333043098 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:22.339039087 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:22.603138924 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:22.603188992 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:22.603786945 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:22.603893042 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:22.608437061 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:22.608462095 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.336218119 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.336345911 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.336400032 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.336442947 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.367258072 CET	49696	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.367310047 CET	443	49696	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.432737112 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.432800055 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.432889938 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.433921099 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.433958054 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.499929905 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.500080109 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.500830889 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.500854969 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.518388987 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.518415928 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.694819927 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.694914103 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.694967031 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.695353031 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.701019049 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.701715946 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.701766014 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.701791048 CET	443	49697	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:23.704377890 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.712850094 CET	49697	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:23.712898970 CET	443	49697	104.16.53.48	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 14:36:24.341213942 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:24.341284990 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:24.341403008 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:24.342258930 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:24.342287064 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:24.425365925 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:24.425596952 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:24.426661015 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:24.426680088 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:24.443453074 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:24.443486929 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.382792950 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.382870913 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.382909060 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.382956982 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.382956982 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.383004904 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.384213924 CET	49698	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.384246111 CET	443	49698	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.434571028 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.434627056 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.434736967 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.435261011 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.435282946 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.512198925 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.514023066 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.514806986 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.514825106 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.520051956 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.520066977 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558515072 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558629036 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558747053 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558780909 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.558804035 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558851004 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558860064 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.558860064 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.558876038 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558927059 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.558937073 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558954000 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.558995008 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.559501886 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.559607029 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.559674978 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.559691906 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.559732914 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.559743881 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.560225010 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.560269117 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.560334921 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.560334921 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.560354948 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.561136007 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.561206102 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.561212063 CET	49699	443	192.168.2.5	104.16.53.48
Mar 20, 2023 14:36:25.561229944 CET	443	49699	104.16.53.48	192.168.2.5
Mar 20, 2023 14:36:25.561254978 CET	49699	443	192.168.2.5	104.16.53.48

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Mar 20, 2023 14:36:22.142857075 CET	56894	53	192.168.2.5	8.8.8.8
Mar 20, 2023 14:36:22.164997101 CET	53	56894	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Mar 20, 2023 14:36:22.142857075 CET	192.168.2.5	8.8.8.8	0xca78	Standard query (0)	www.mediafire.com	A (IP address)	IN (0x0001)	false

DNS Answers

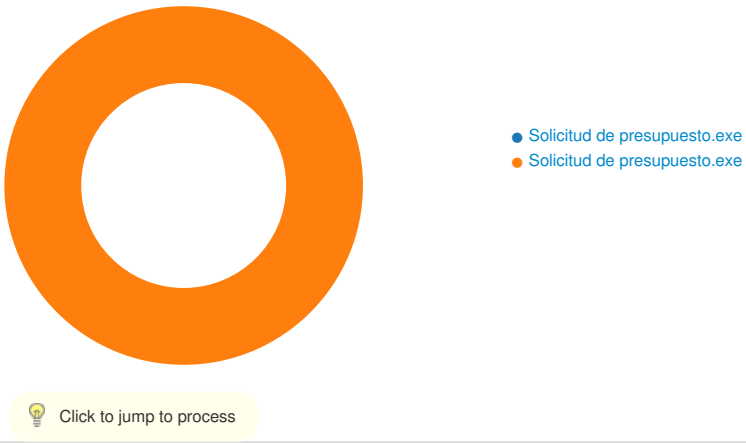
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Mar 20, 2023 14:36:22.164997101 CET	8.8.8.8	192.168.2.5	0xca78	No error (0)	www.mediafire.com		104.16.53.48	A (IP address)	IN (0x0001)	false
Mar 20, 2023 14:36:22.164997101 CET	8.8.8.8	192.168.2.5	0xca78	No error (0)	www.mediafire.com		104.16.54.48	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.mediafire.com

Statistics

Behavior



System Behavior

Analysis Process: Solicitud de presupuesto.exe PID: 5800, Parent PID: 3324

General

Target ID:	0
Start time:	14:35:19
Start date:	20/03/2023

Path:	C:\Users\user\Desktop\Solicitud de presupuesto.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Solicitud de presupuesto.exe
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	E6F54CE2BE4854FDCA9C97450C347A2C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000000.307522232.000000000040D000.00000020.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000000.00000002.404604650.000000000040D000.00000020.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems)
Reputation:	low

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Solicitud de presupuesto.exe PID: **1352**, Parent PID: **5800**

General

Target ID:	1
Start time:	14:36:04
Start date:	20/03/2023
Path:	C:\Users\user\Desktop\Solicitud de presupuesto.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Solicitud de presupuesto.exe
Imagebase:	0x400000
File size:	86016 bytes
MD5 hash:	E6F54CE2BE4854FDCA9C97450C347A2C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: LokiBot_Dropper_Packed_R11_Feb18, Description: Auto-generated rule - file scan copy.pdf.r11, Source: 00000001.00000000.403982899.000000000040D000.00000020.00000001.01000000.00000003.sdmp, Author: Florian Roth (Nextron Systems) • Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000001.00000002.575875706.0000000000560000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

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	564400	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	564400	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	564400	InternetOpenUrlA

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	564400	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	564400	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	564400	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly