ID: 395374
Sample Name: yiu0bguw4d
Cookbook: default.jbs
Time: 13:15:22
Date: 22/04/2021
Version: 31.0.0 Emerald

Table of Contents

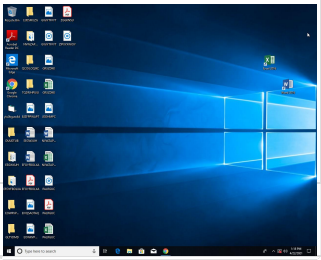
Analysis Report yiu0bguw4d

Overview

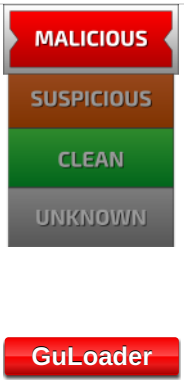
General Information

Sample Name:	yiu0bguw4d (renamed file extension from none to exe)
Analysis ID:	395374
MD5:	d5b8e2ce449917..
SHA1:	fe872c03ceef394..
SHA256:	981d483b809a8d..
Tags:	GuLoader
Infos:	

Most interesting Screenshot:



Detection

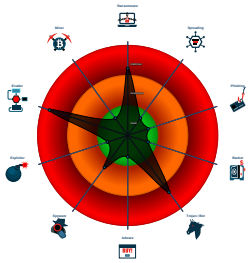


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Contains functionality to hide a threa…
- Detected RDTSC dummy instruction…
- Hides threads from debuggers
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…

Classification



Startup

- **System is w10x64**
- yiu0bguw4d.exe (PID: 204 cmdline: 'C:\Users\user\Desktop\yiu0bguw4d.exe' MD5: D5B8E2CE449917BF395454082DE6CBA9)
  - RegAsm.exe (PID: 6304 cmdline: 'C:\Users\user\Desktop\yiu0bguw4d.exe' MD5: 6FD7592411112729BF6B1F2F6C34899F)
    - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=1dMb_B0qeMj8gz7LWq1fB7I-0h8qhomgl",
  "Injection Process": [
    "RegAsm.exe",
    "RegSvcs.exe",
    "MSBuild.exe"
  ]
}
```

Yara Overview

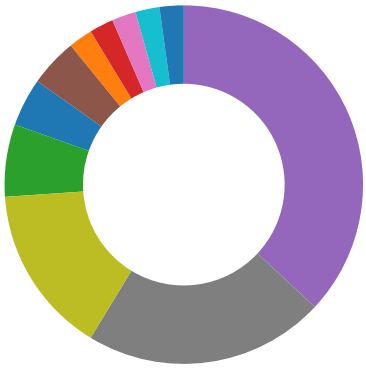
Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.494899061.0000000000A00000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: RegAsm.exe PID: 6304	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
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Networking:

C2 URLs / IPs found in malware configuration

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

Detected RDTSC dummy instruction sequence (likely for instruction hammering)

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:

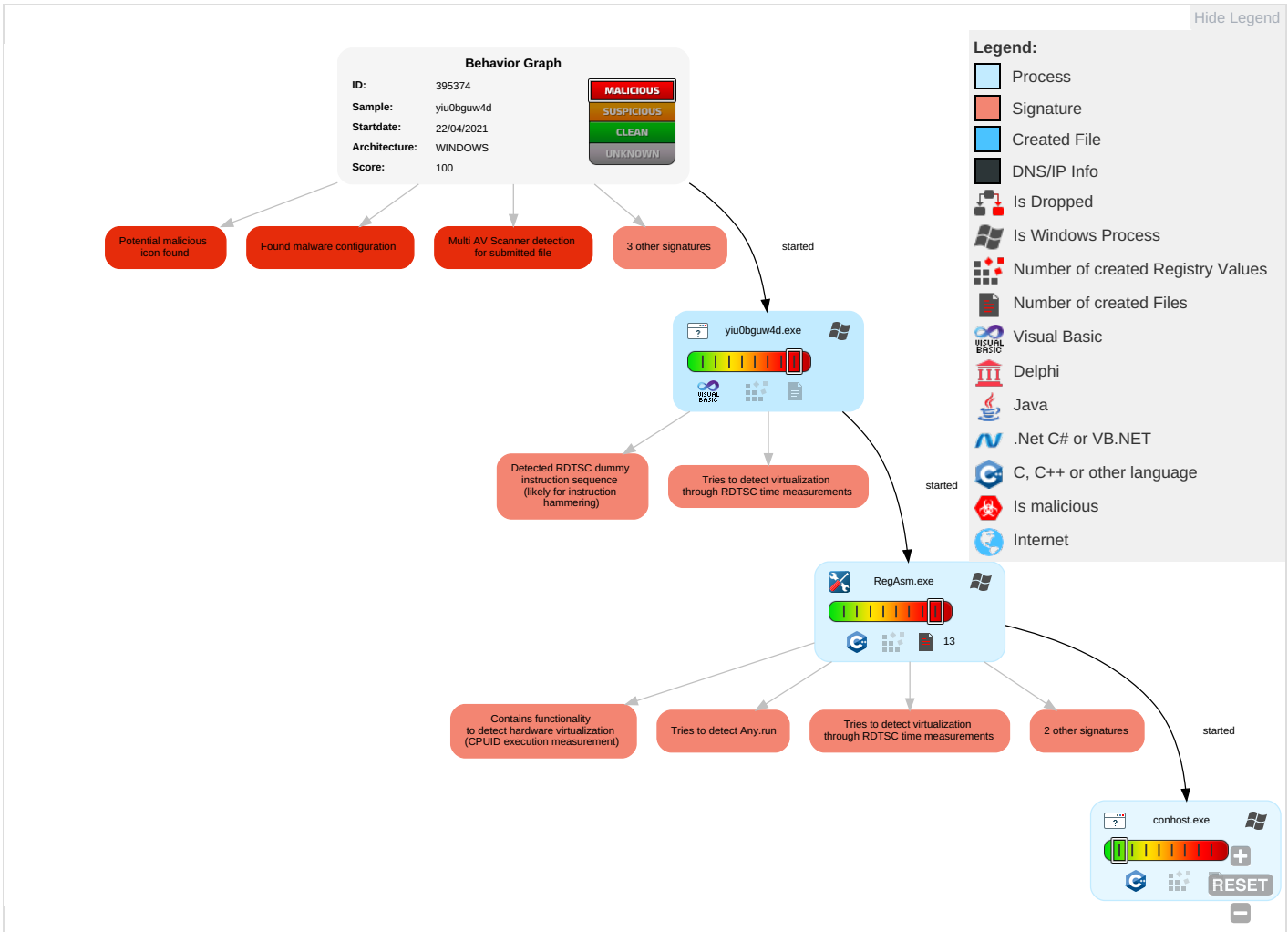
Contains functionality to hide a thread from the debugger

Hides threads from debuggers

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Re Se Ef
Valid Accounts	Windows Management Instrumentation	DLL Side-Loading 1	Process Injection 2	Virtualization/Sandbox Evasion 2 2	Input Capture 1	Security Software Discovery 7 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Application Layer Protocol 1	Eavesdrop on Insecure Network Communication	Re Tr W Au
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Process Injection 2	LSASS Memory	Virtualization/Sandbox Evasion 2 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phone Calls/SMS	Re W W Au
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	Ol De Cl Ba
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	DLL Side-Loading 1	NTDS	System Information Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 2	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

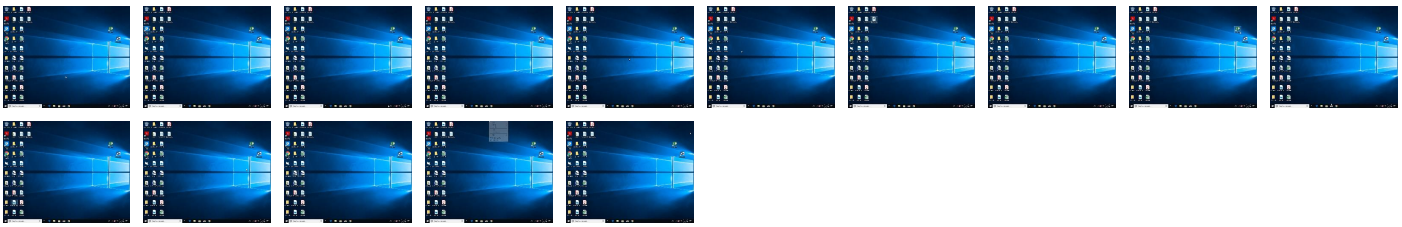
Behavior Graph



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
yiu0bguw4d.exe	62%	Virustotal		Browse
yiu0bguw4d.exe	26%	Metadefender		Browse
yiu0bguw4d.exe	79%	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

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	395374
Start date:	22.04.2021
Start time:	13:15:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 42s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yiu0bguw4d (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	22
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.rans.troj.evad.winEXE@3/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 7% (good quality ratio 5.3%) • Quality average: 42.1% • Quality standard deviation: 25.8%
HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

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, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 13.88.21.125, 131.253.33.200, 13.107.22.200, 40.88.32.150, 20.82.210.154, 92.122.145.220, 13.64.90.137, 184.30.24.56, 8.241.126.249, 8.253.145.121, 8.241.78.254, 8.241.90.126, 8.238.27.126, 20.50.102.62, 142.250.185.110, 92.122.213.247, 92.122.213.194, 20.54.26.129 • Excluded domains from analysis (whitelisted): 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, skypedataprdcoleus15.cloudapp.net, e12564.dspb.akamaiedge.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, drive.google.com, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus15.cloudapp.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
13:17:14	API Interceptor	181x 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):	5.766092447013738
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:	yiu0bguw4d.exe
File size:	159744
MD5:	d5b8e2ce449917bf395454082de6cba9
SHA1:	fe872c03ceef39422218003bc5a34be4faf47e55
SHA256:	981d483b809a8d146115d1a1feb7bb8d588e014a0f009d b528662d39f5657e4
SHA512:	54dc37f2345a4b70786920c80adf8c1fc72c9ab97edf95b 239453c081ab221134fbbc8ae8d8fd3ce635d4b3aec8f42 fbc44005930e917e10e1a72cbd5e442e48
SSDEEP:	3072:q9gtPOO/XUh8LKcLMD8bvl2Zo/NK9HRQBxEvO K69GqcOUVA9DrBH8YdKHar3dSGE:q9yjkz3DYYZo/Q 9xQBxEvOK69GqfUVAr
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....6...W... W...W...K...W...u...W...q...W..Rich.W.....PE ..L...../L.....@...`.....P....@

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4017e8
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:	0x4C2F1AF0 [Sat Jul 3 11:11:44 2010 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	66c809d2e31d4e6411dd9b96c6b12187

Entrypoint Preview

Instruction
push 00401A08h
call 00007FC0949B6855h
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 [edx], dh
pushfd
movsd
popad
pop es
hlt
loopne 00007FC0949B68AFh
mov byte ptr [edx-7CF2A144h], cl
add al, byte ptr [00000000h]
add byte ptr [eax], al
add dword ptr [eax], eax
add byte ptr [eax], al
add byte ptr [eax], al
fcomp st(0), st(7)
sbb eax, dword ptr [ebx]
push eax
jc 00007FC0949B68D1h
push 00000065h
arpl word ptr [ecx+esi+00h], si
or byte ptr [ecx+00h], al
and byte ptr [eax], cl
inc ecx
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
add eax, E18115F3h
add al, 01h
mov dword ptr [ecx-4Ah], eax
push es
xor dword ptr [ebp-1Ch], ebp
inc ecx
jc 00007FC0949B6819h
mov ecx, dword ptr [ebx+5Fh]
dec esi
clc
retf
dec ebp
adc dword ptr [edi-48h], 76h
adc byte ptr [4F3A912Eh], bl
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]

Instruction
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
pop ss
add dword ptr [eax], eax
add byte ptr [eax+eax+00h], dl
add byte ptr [eax], al
or al, 00h
jne 00007FC0949B68C6h
jnc 00007FC0949B68C3h
outsb
jc 00007FC0949B68CCh
outsb
jc 00007FC0949B6864h
or eax, 54000D01h
popad

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x23ab4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2a000	0x9b4	.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	0x238	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.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	0x23130	0x24000	False	0.419569227431	data	6.02803482745	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x25000	0x460c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x2a000	0x9b4	0x1000	False	0.17724609375	data	2.10021451926	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2a884	0x130	data		
RT_ICON	0x2a59c	0x2e8	data		
RT_ICON	0x2a474	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x2a444	0x30	data		
RT_VERSION	0x2a150	0x2f4	data		

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaVarForInit, __vbaObjSet, __vbaOnError, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaErase, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaVarTstEq, __vbaObjVar, __vbaI2I4, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRedim, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaVar2Vec, __vbaR8Str, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, __vbaDerefAry1, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarDup, __vbaStrToAnsi, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, __vbaFPInt, __vbaVarForNext, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Vought
InternalName	Uruguayanernes5
FileVersion	1.00
CompanyName	Vought
LegalTrademarks	Vought
Comments	Vought
ProductName	Vought
ProductVersion	1.00
FileDescription	Vought
OriginalFilename	Uruguayanernes5.exe

Network Behavior

UDP Packets

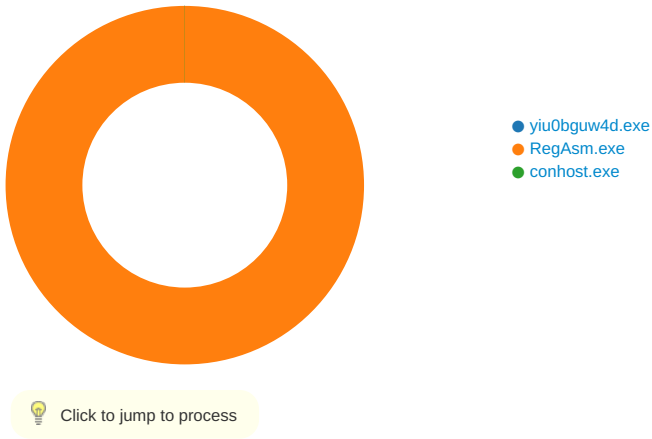
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2021 13:16:04.022247076 CEST	65307	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:04.071670055 CEST	53	65307	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:05.343327999 CEST	64344	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:05.369664907 CEST	62060	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:05.402415037 CEST	53	64344	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:05.406553984 CEST	61805	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:05.419886112 CEST	53	62060	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:05.457952023 CEST	53	61805	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:06.622735977 CEST	54795	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:06.671664953 CEST	53	54795	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:08.462213993 CEST	49557	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:08.521538019 CEST	53	49557	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:09.191998959 CEST	61733	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:09.243575096 CEST	53	61733	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:11.151460886 CEST	65447	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:11.203442097 CEST	53	65447	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:12.230552912 CEST	52441	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:12.285553932 CEST	53	52441	8.8.8.8	192.168.2.5

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2021 13:16:15.510654926 CEST	62176	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:15.562283039 CEST	53	62176	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:16.340872049 CEST	59596	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:16.389904022 CEST	53	59596	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:17.944291115 CEST	65296	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:17.995753050 CEST	53	65296	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:19.297769070 CEST	63183	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:19.346590996 CEST	53	63183	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:20.653418064 CEST	60151	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:20.702169895 CEST	53	60151	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:21.551079988 CEST	56969	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:21.611035109 CEST	53	56969	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:32.704593897 CEST	55161	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:32.763308048 CEST	53	55161	8.8.8.8	192.168.2.5
Apr 22, 2021 13:16:59.578900099 CEST	54757	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:16:59.639167070 CEST	53	54757	8.8.8.8	192.168.2.5
Apr 22, 2021 13:17:02.901556015 CEST	49992	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:17:02.950134039 CEST	53	49992	8.8.8.8	192.168.2.5
Apr 22, 2021 13:17:14.093085051 CEST	60075	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:17:14.162861109 CEST	53	60075	8.8.8.8	192.168.2.5
Apr 22, 2021 13:17:24.351308107 CEST	55016	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:17:24.409837008 CEST	53	55016	8.8.8.8	192.168.2.5
Apr 22, 2021 13:17:56.500247955 CEST	64345	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:17:56.548854113 CEST	53	64345	8.8.8.8	192.168.2.5
Apr 22, 2021 13:18:17.169271946 CEST	57128	53	192.168.2.5	8.8.8.8
Apr 22, 2021 13:18:17.236749887 CEST	53	57128	8.8.8.8	192.168.2.5

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: yiu0bguw4d.exe PID: 204 Parent PID: 5564

General

Start time:	13:16:11
Start date:	22/04/2021
Path:	C:\Users\user\Desktop\yiu0bguw4d.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yiu0bguw4d.exe'
Imagebase:	0x400000
File size:	159744 bytes
MD5 hash:	D5B8E2CE449917BF395454082DE6CBA9
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

Analysis Process: RegAsm.exe PID: 6304 Parent PID: 204

General

Start time:	13:17:00
Start date:	22/04/2021
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yiu0bguw4d.exe'
Imagebase:	0x610000
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: 0000000B.00000002.494899061.0000000000A00000.00000040.00000001.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	A045A7	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	A045A7	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	A045A7	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	A045A7	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
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	A045A7	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	A045A7	InternetOpenUrlA

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: 6344 Parent PID: 6304

General

Start time:	13:17:02
Start date:	22/04/2021
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