ID: 377275
Sample Name:
Zahlung_03242021_jpg.scr
Cookbook: default.jbs
Time: 11:15:38
Date: 29/03/2021
Version: 31.0.0 Emerald

Table of Contents

Copyright Joe Security LLC 2021

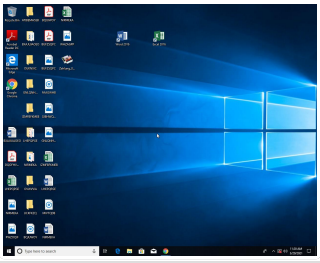
Analysis Report Zahlung_03242021_jpg.scr

Overview

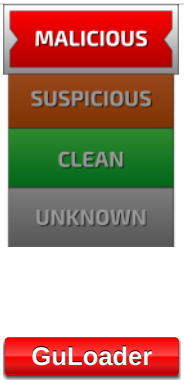
General Information

Sample Name:	Zahlung_03242021_jpg.scr (renamed file extension from scr to exe)
Analysis ID:	377275
MD5:	6540b24ec7d131..
SHA1:	2c29267c98ff52b..
SHA256:	ea36f17e9a118b5.
Infos:	

Most interesting Screenshot:



Detection

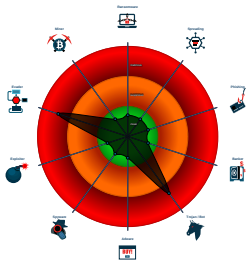


Score:	76
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Contains functionality to detect hard…
- Found potential dummy code loops (…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage
- Contains functionality for execution …
- Contains functionality to read the PEB
- Found large amount of non-executed…
- PE file contains strange resources
- Program does not show much activi…

Classification



Startup

- **System is w10x64**
- Zahlung_03242021_jpg.exe (PID: 6464 cmdline: 'C:\Users\user\Desktop\Zahlung_03242021_jpg.exe' MD5: 6540B24EC7D131CCBC57624915F9180C)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

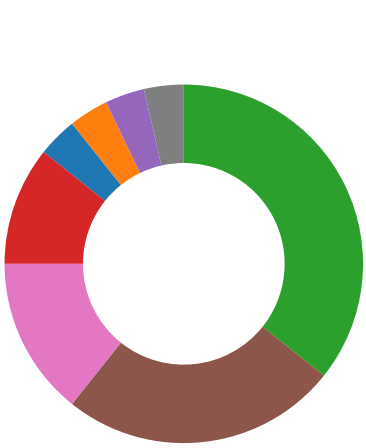
Source	Rule	Description	Author	Strings
Process Memory Space: Zahlung_03242021_jpg.exe PID: 6464	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Zahlung_03242021_jpg.exe PID: 6464	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview

Copyright Joe Security LLC 2021



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

Contains functionality to detect hardware virtualization (CPUID execution measurement)

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

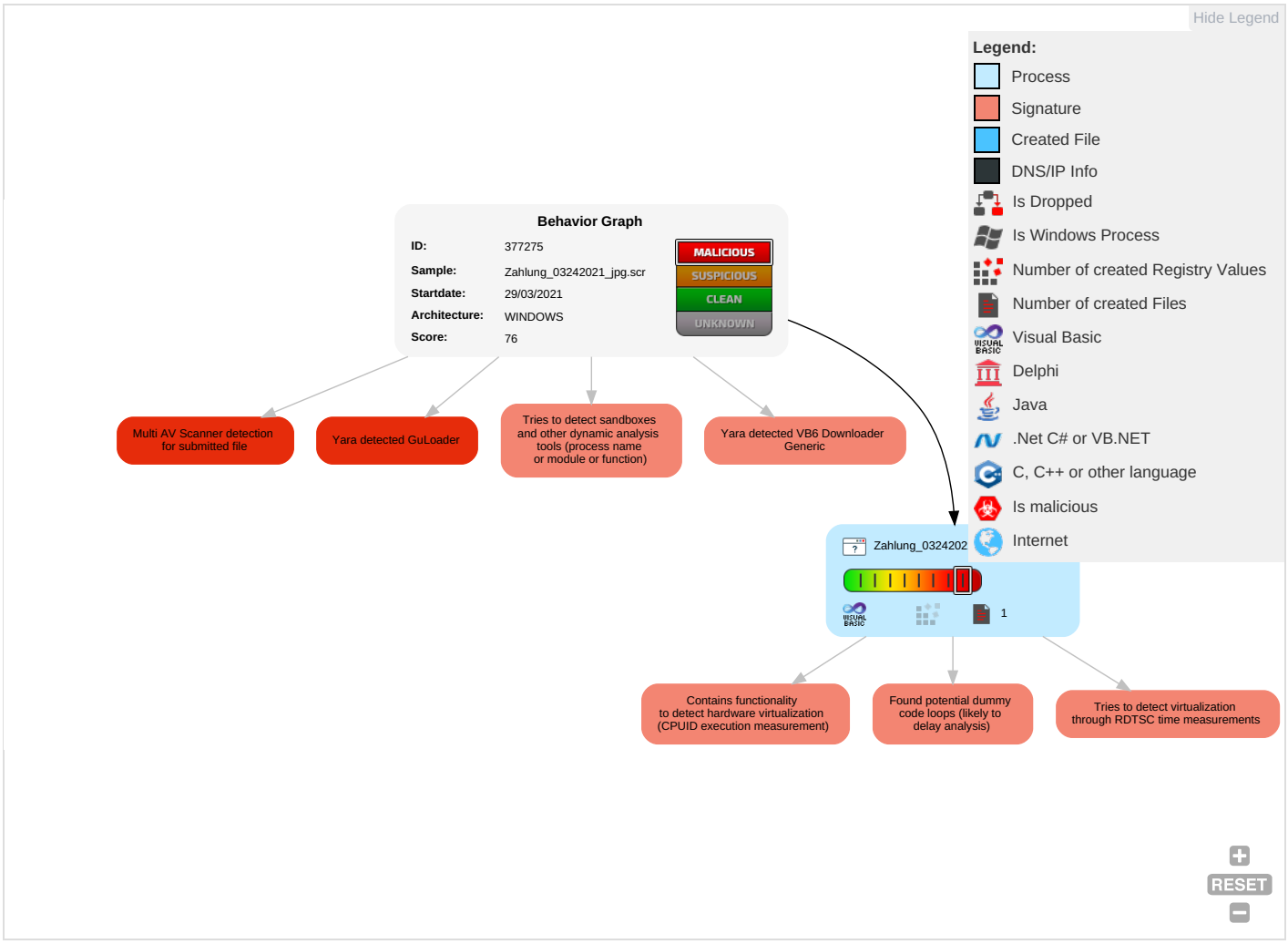
Found potential dummy code loops (likely to delay analysis)

Mitre Att&ck Matrix

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

Behavior Graph

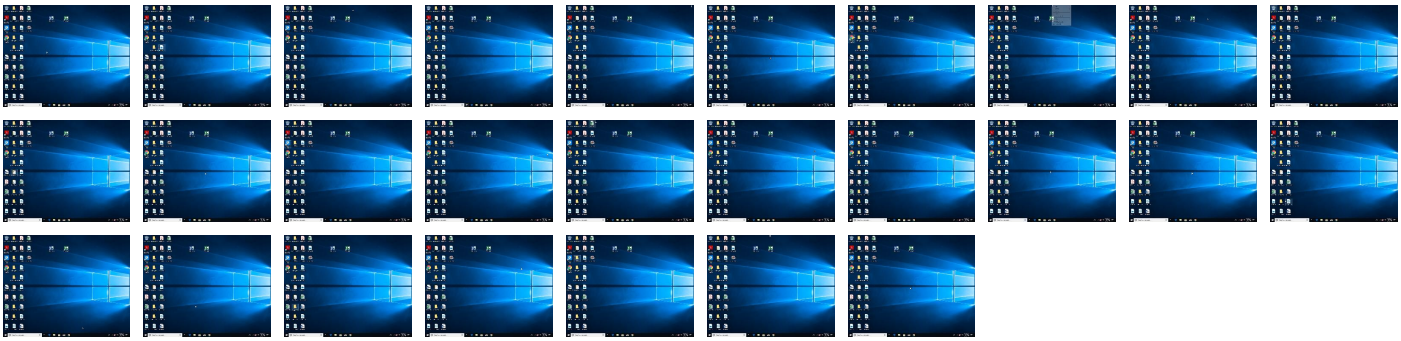
Copyright Joe Security LLC 2021



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
Zahlung_03242021_jpg.exe	64%	Virustotal		Browse
Zahlung_03242021_jpg.exe	24%	Metadefender		Browse
Zahlung_03242021_jpg.exe	76%	ReversingLabs	Win32.Trojan.Vebzenpak	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Copyright Joe Security LLC 2021

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:	377275
Start date:	29.03.2021
Start time:	11:15:38
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 54s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Zahlung_03242021_jpg.scr (renamed file extension from scr 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:	8
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:	mal76.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	5.420240325918891
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:	Zahlung_03242021_jpg.exe
File size:	98304
MD5:	6540b24ec7d131ccbc57624915f9180c
SHA1:	2c29267c98ff52bb6a44e3e3dca1c0d1c668c870
SHA256:	ea36f17e9a118b567da5b9be48f13527cdd109da17d5e5a bb0809f9356622f9b
SHA512:	9228c775e816af94b385b3ca03a43653c8fc8ff674c03b5 bd4fb8ebf071eb55099b8eca30e9fc8001a2aee88cf00d0 4a656c9ee536fa03655eebe2889f8154fa
SSDEEP:	1536:8g9twd+oMfleXcQ2T9gg86snOuC194pnLbl8Xc0E ew04nPai0Kt:8nQeXoT1W19259i0
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...B...B...B..L^...B...`...B...d...B..Rich.B.....PE..L....6_P.....@...@.....P....@.....

File Icon

Icon Hash:	11d0ecac88e43480

Static PE Info

General

Entrypoint:	0x4015b0
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:	0x505F36E5 [Sun Sep 23 16:20:53 2012 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:	0ecd972e837a1a17658b43cce3314253

Entrypoint Preview

Instruction
push 00402E74h
call 00007FDEA05C1F93h
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 bh, dh
retn E273h
and ch, byte ptr [edi-6366BBE6h]
sub al, 6Eh
in eax, dx
sub dword ptr [edi+60h], ebp
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
and byte ptr [eax], ah
and byte ptr [eax], ah
and byte ptr [eax], ah
inc esi
dec esp
pop ecx
push esi
inc ebp
inc esp
pop ecx
inc edi
push esp
dec ecx
inc edi
add byte ptr [ebx+69h], dh
imul ebp, dword ptr [ebx+00h], 00h
add byte ptr [eax], al
dec esp
xor dword ptr [eax], eax

Copyright Joe Security LLC 2021

Instruction
or ebx, dword ptr [ebp+46h]
jnp 00007FDEA05C1F55h
idiv byte ptr [esi+esi*2]
inc ebx
mov eax, 4224415Bh
adc al, 3Ch
or ebp, ecx
adc dword ptr [ebx-444A3438h], edx
dec edx
mov cl, 90h
push FFFFFFCBh
pop ebx
sbb al, C6h
fstsw word ptr [edx]
dec edi
lodsd
xor ebx, dword ptr [ecx-48EE309Ah]
or al, 00h
stosb
add byte ptr [eax-2Dh], ah
xchg eax, ebx
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
push eax
pop ss
add byte ptr [eax], al
adc ax, 00000000h
add byte ptr [74654700h], al
push 010D0065h
or al, 00h
jc 00007FDEA05C200Ch
je 00002016h
imul ebp, dword ptr [ebx+6Bh], 00000065h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x13ff4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x17000	0x1958	.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	

Copyright Joe Security LLC 2021

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x228	0x20	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x178	.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	0x135cc	0x14000	False	0.362646484375	data	5.77045811117	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x15000	0x120c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x17000	0x1958	0x2000	False	0.516723632812	data	4.53448005224	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x180b0	0x8a8	data		
RT_ICON	0x179e8	0x6c8	data		
RT_ICON	0x17480	0x568	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x17450	0x30	data		
RT_VERSION	0x17150	0x300	data	Telugu	India

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaStrVarMove, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaStrCat, __vbaSetSystemError, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryVar, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaVarTstLt, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, __vbaStrToUnicode, _adj_fprem, _adj_fdivr_m64, __vbaVarErrI4, __vbaFPException, __vbaUbound, __vbaDateVar, _CIlog, __vbaErrorOverflow, __vbaNew2, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaVarAdd, __vbaVarDup, __vbaStrToAnsi, _CIatan, __vbaStrMove, __vbaCastObj, __vbaAryCopy, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x044a 0x04b0
LegalCopyright	Copyright MateFar
InternalName	Confidency
FileVersion	3.00
CompanyName	MateFar
LegalTrademarks	Copyright MateFar
ProductName	uncatechizedness
ProductVersion	3.00
FileDescription	MateFar
OriginalFilename	Confidency.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Telugu	India	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Zahlung_03242021_jpg.exe PID: 6464 Parent PID: 5996

General

Start time:	11:16:19
Start date:	29/03/2021
Path:	C:\Users\user\Desktop\Zahlung_03242021_jpg.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Zahlung_03242021_jpg.exe'
Imagebase:	0x400000
File size:	98304 bytes
MD5 hash:	6540B24EC7D131CCBC57624915F9180C
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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis