ID: 356750
Sample Name: Order 3350191107102300.bat.exe
Cookbook: default.jbs
Time: 15:58:25
Date: 23/02/2021
Version: 31.0.0 Emerald

Table of Contents

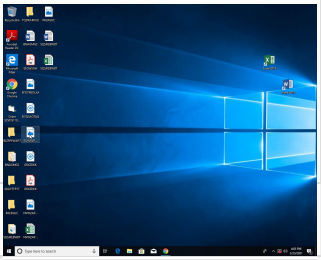
Analysis Report Order 3350191107102300.bat.exe

Overview

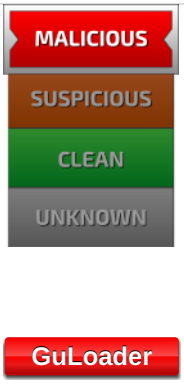
General Information

Sample Name:	Order 3350191107102300.bat.exe
Analysis ID:	356750
MD5:	7e7df58fd2de6dd..
SHA1:	6d2753aa52a782..
SHA256:	96861b47729d7e..
Tags:	exe GuLoader
Infos:	

Most interesting Screenshot:



Detection



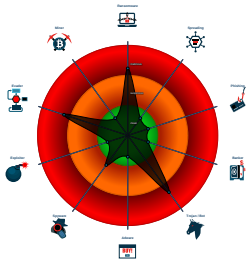
GuLoader

Score:	80
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected GuLoader
- Initial sample is a PE file and has a …
- 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
- Creates a DirectInput object (often fo…
- Detected potential crypto function

Classification



Startup

- **System is w10x64**
- Order 3350191107102300.bat.exe (PID: 3276 cmdline: 'C:\Users\user\Desktop\Order 3350191107102300.bat.exe' MD5: 7E7DF58FD2DE6DDDAE514D65A55EA92D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

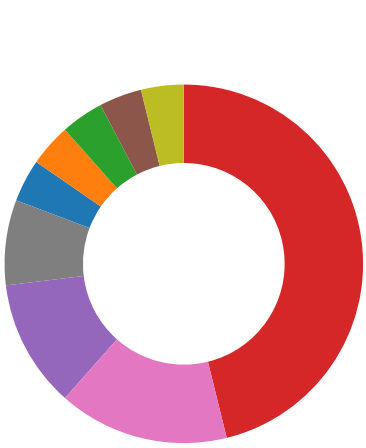
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: Order 3350191107102300.bat.exe PID: 3276	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: Order 3350191107102300.bat.exe PID: 3276	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Compliance:

Uses 32bit PE files

System Summary:

Potential malicious icon found

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Malware Analysis System Evasion:

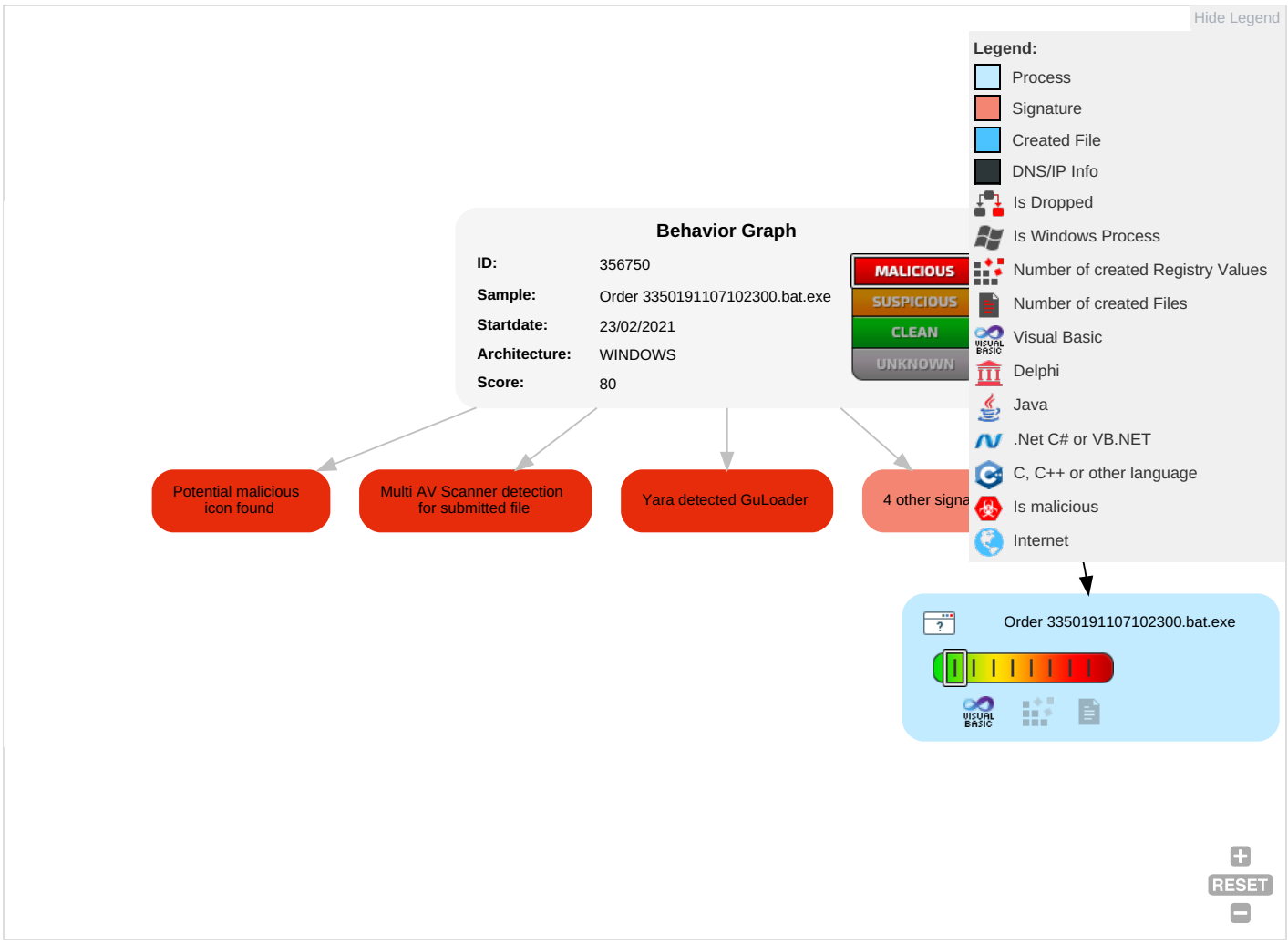
Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

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
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1	Process Injection 1	Input Capture 1	Security Software Discovery 2 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Obfuscated Files or Information 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

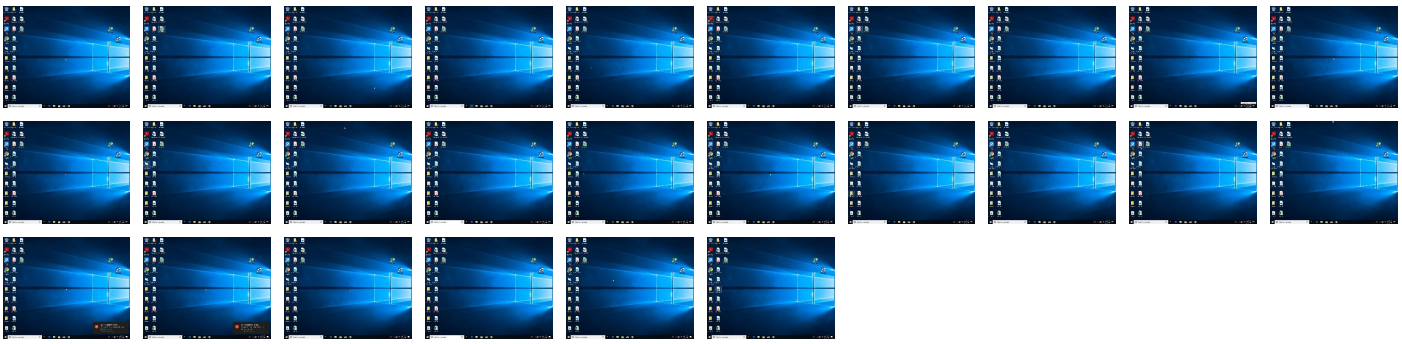
Behavior Graph



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
Order 3350191107102300.bat.exe	39%	Virustotal		Browse
Order 3350191107102300.bat.exe	38%	ReversingLabs	Win32.Trojan.VBObfuse	

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:	356750
Start date:	23.02.2021
Start time:	15:58:25
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Order 3350191107102300.bat.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:	35
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:	mal80.rans.troj.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19% (good quality ratio 15.8%) • Quality average: 44.5% • Quality standard deviation: 30.1%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, HxTsr.exe, RuntimeBroker.exe, WMIADAP.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.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):	4.8128892871742375
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:	Order 3350191107102300.bat.exe
File size:	61440
MD5:	7e7df58fd2de6dddae514d65a55ea92d
SHA1:	6d2753aa52a78273a1aad5b9f9aaa422395a80d4
SHA256:	96861b47729d7e9e4af5c1b016900631339c8357a614cf4fb02ebfbbadece8ff
SHA512:	bb4a337359fe81136e12bea5d9cefbfedb1ae402b17962a8a07a26e47d0ead672228652f8c9111609ccc191f8cbbfb6a9a7facced83bec958a61b807e13a48d9
SSDEEP:	768:5Zs/yUcqX46IjPAygxo9N/hZLbimvoZO1diPdn0hscFmR:Ino62Poxo9jZv7+O6FwK
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....S^U.....0.....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x4012c4
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:	0x555E53E2 [Thu May 21 21:53:38 2015 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:	f8fb5be8a6ea86fb9d04da61d8bfeb3a

Entrypoint Preview

Instruction
push 00401500h
call 00007F2BA0AB00A3h
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
cmp byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
cmp eax, 4D9D86E1h
hlt
jnp 00007F2BA0AB0100h
stosb
fstsw word ptr [eax+ebx-1Fh]
stosd
loope 00007F2BA0AB0090h
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
add byte ptr [eax], al
enter FE93h, 02h
push esp
jns 00007F2BA0AB011Dh
insd
insb
add byte ptr [esi], bh
add byte ptr [eax], al
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
pop es

Instruction
fnclex
pop ss
pop esp
jnl 00007F2BA0AB0080h
jmp 00007F2BA0AB00F4h
cwde
pop ss
inc esp
inc edx
fsubr st(0), st(0)
mov ebx, dword ptr [ebx]
out 57h, eax
sub esi, edi
enter 442Dh, 47h
and byte ptr [edx-14D2B208h], 00000057h
push cs
cmp cl, byte ptr [edi-53h]
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
nop
add dword ptr [eax], eax
add byte ptr [eax+eax+00h], cl
add byte ptr [eax], al
push es
add byte ptr [ecx+6Dh], ah
popad
outsb
jne 00007F2BA0AB0117h
add byte ptr [4D000C01h], cl
outsd
outsb
outsd
jo 00007F2BA0AB0125h
jns 00007F2BA0AB0115h
push 00397369h
sbb dword ptr [ecx], eax
add byte ptr [edx+00h], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc214	0x28	.text

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xf000	0x99c	.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	0xd0	.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	0xb5e8	0xc000	False	0.462443033854	data	5.52315767674	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0xd000	0x118c	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0xf000	0x99c	0x1000	False	0.178955078125	data	2.08945288854	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xf86c	0x130	data		
RT_ICON	0xf584	0x2e8	data		
RT_ICON	0xf45c	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xf42c	0x30	data		
RT_VERSION	0xf150	0x2dc	data	Hungarian	Hungary

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaAryMove, __vbaFreeVar, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, _adj_fdivr_m16i, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaErrorOverflow, __vbaNew2, __vbaVar2Vec, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaVarDup, _CIatan, __vbaCastObj, _allmul, _CItan, _CIexp, __vbaFreeObj, __vbaFreeStr

Version Infos

Description	Data
Translation	0x040e 0x04b0
LegalCopyright	Copyright (C) AC
InternalName	CODFISH
FileVersion	1.00
CompanyName	AC
LegalTrademarks	Copyright (C) AC
Comments	AC
ProductName	AC
ProductVersion	1.00
FileDescription	AC
OriginalFilename	CODFISH.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map

Language of compilation system	Country where language is spoken	Map
Hungarian	Hungary	

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: Order 3350191107102300.bat.exe PID: 3276 Parent PID: 5556

General

Start time:	15:59:10
Start date:	23/02/2021
Path:	C:\Users\user\Desktop\Order 3350191107102300.bat.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Order 3350191107102300.bat.exe'
Imagebase:	0x400000
File size:	61440 bytes
MD5 hash:	7E7DF58FD2DE6DDDAE514D65A55EA92D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

Code Analysis