ID: 392084
Sample Name: KOPEKER.exe
Cookbook: default.jbs
Time: 08:41:50
Date: 19/04/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report KOPEKER.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Startup 4
Malware Configuration 4
Threatname: GuLoader 4
Yara Overview 4
Memory Dumps 4
Sigma Overview 5
Signature Overview 5
AV Detection: 5
Networking: 5
Data Obfuscation: 5
Hooking and other Techniques for Hiding and Protection: 5
Malware Analysis System Evasion: 5
Anti Debugging: 5
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 6
Thumbnails 6
Antivirus, Machine Learning and Genetic Malware Detection 7
Initial Sample 7
Dropped Files 7
Unpacked PE Files 8
Domains 8
URLs 8
Domains and IPs 8
Contacted Domains 8
Contacted IPs 8
General Information 8
Simulations 9
Behavior and APIs 9
Joe Sandbox View / Context 9
IPs 9
Domains 9
ASN 9
JA3 Fingerprints 9
Dropped Files 9
Created / dropped Files 9
Static File Info 9
General 9
File Icon 10
Static PE Info 10
General 10
Entrypoint Preview 10
Data Directories 11
Sections 11
Resources 11
Imports 12
Version Infos 12
Possible Origin 12
Network Behavior 12

Copyright Joe Security LLC 2021

Code Manipulations 12
Statistics 12
System Behavior 12
Analysis Process: KOPEKER.exe PID: 5760 Parent PID: 5856 12
General 12
File Activities 13
Disassembly 13
Code Analysis 13

Copyright Joe Security LLC 2021

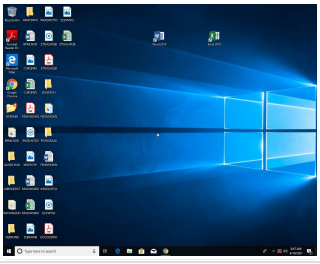
Analysis Report KOPEKER.exe

Overview

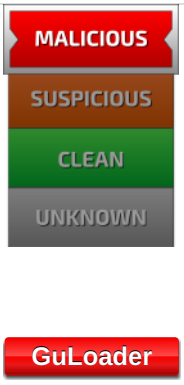
General Information

Sample Name:	KOPEKER.exe
Analysis ID:	392084
MD5:	cd885321b35b73..
SHA1:	2f09e0eb93927d8.
SHA256:	495edfb60c0a9af..
Infos:	

Most interesting Screenshot:



Detection



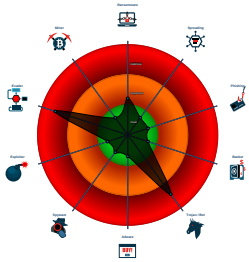
GuLoader

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

Signatures

- Found malware configuration
- Icon mismatch, binary includes an ic…
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- C2 URLs / IPs found in malware con…
- Contains functionality to detect hard…
- Detected RDTSC dummy instruction…
- Found potential dummy code loops (…
- Machine Learning detection for samp…
- Tries to detect sandboxes and other…
- Tries to detect virtualization through…
- Yara detected VB6 Downloader Gen…
- Abnormal high CPU Usage

Classification



Startup

- **System is w10x64**
- KOPEKER.exe (PID: 5760 cmdline: 'C:\Users\user\Desktop\KOPEKER.exe' MD5: CD885321B35B73421CD63E3150D677F7)
- **cleanup**

Malware Configuration

Threatname: GuLoader

```
{
  "Payload URL": "https://drive.google.com/uc?export=download&id=13mbmc5DER0_wKkBDGQL230MFPs1cTVbi",
  "Injection Process": [
    "RegAsm.exe",
    "RegSvcs.exe",
    "MSBuild.exe"
  ]
}
```

Yara Overview

Memory Dumps

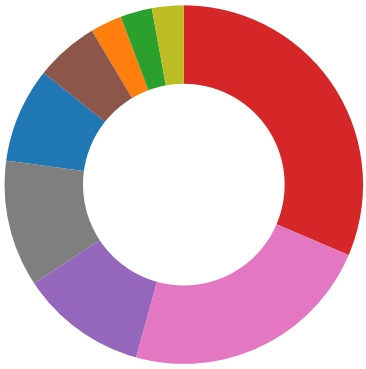
Source	Rule	Description	Author	Strings
00000000.00000002.985827741.000000000620000.00000040.00000001.sdmp	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: KOPEKER.exe PID: 5760	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: KOPEKER.exe PID: 5760	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	

Copyright Joe Security LLC 2021

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

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

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

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

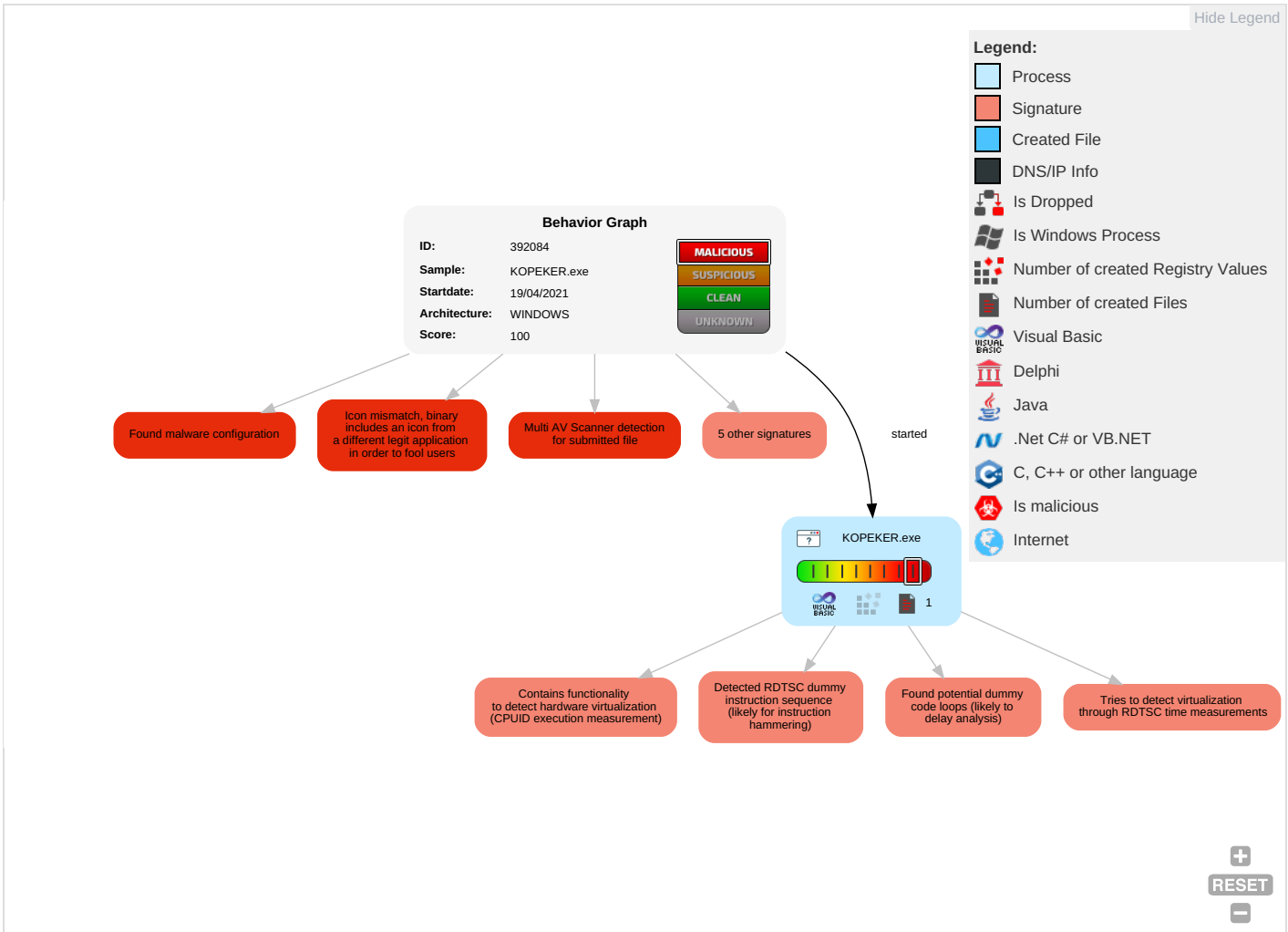
Found potential dummy code loops (likely to delay analysis)

Copyright Joe Security LLC 2021

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	Masquerading 1	OS Credential Dumping	Security Software Discovery 5 1 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication	R T W A
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Virtualization/Sandbox Evasion 1 1	LSASS Memory	Virtualization/Sandbox Evasion 1 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Application Layer Protocol 1	Exploit SS7 to Redirect Phone Calls/SMS	R W W A
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 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)	Obfuscated Files or Information 1	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap	
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	System Information Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication	

Behavior Graph

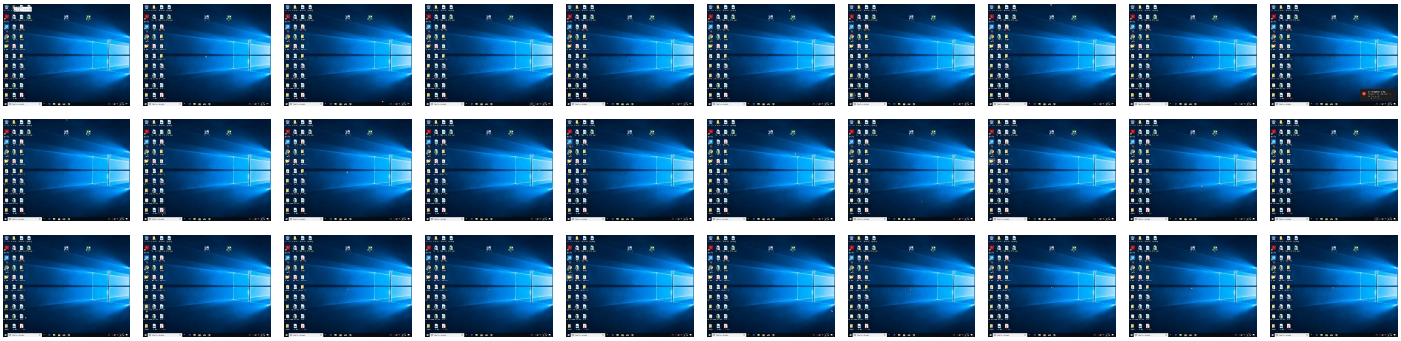


Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Copyright Joe Security LLC 2021



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
KOPEKER.exe	62%	Virustotal		Browse
KOPEKER.exe	38%	Metadefender		Browse
KOPEKER.exe	83%	ReversingLabs	Win32.Trojan.VBObfuse	
KOPEKER.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Copyright Joe Security LLC 2021

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:	392084
Start date:	19.04.2021
Start time:	08:41:50
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KOPEKER.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:	11
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.troj.evad.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 9.4% (good quality ratio 3.7%) • Quality average: 18.5% • Quality standard deviation: 24%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe

Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, MusNotifyIcon.exe, conhost.exe, svchost.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):	5.7626204591873975
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:	KOPEKER.exe
File size:	118784
MD5:	cd885321b35b73421cd63e3150d677f7
SHA1:	2f09e0eb93927d82076f34549b0d4d3b7b393aab
SHA256:	495edfb60c0a9af0c57251ce28ca0bcf4c911324f59074f99c2797e36c3f3ef4

General

SHA512:	cf8124f2fb91027365cb2ed941b121698a40e5992935bc0b3b6bdd15ad92a417ad62bf247b643132d886145dfcc6c3a48b3ee52aaa6fd8577e4b37457cd83c81
SSDEEP:	1536:q28031a0rd/d7dGBWBWevDWoiLUaYuWMm2IPKtopQYXQHoH5encrFQLn9MamuSHi:qiFa0BGBWYeaoNHKtG+JMi
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.....J.....p...`.....h.....@.....

File Icon

Icon Hash:	c0c6f2e0e4fefe3f

Static PE Info

General

Entrypoint:	0x401968
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:	0x4A88EC80 [Mon Aug 17 05:37:04 2009 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:	7677b40f5f8927412a58af017314f1ed

Entrypoint Preview

Instruction
push 0040F4D8h
call 00007F44BCECE623h
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 [ebx-604C4D3Dh], dl
cmp eax, 0B8E48E7h
imul edi, dword ptr [esi+3Dh], 00FB3ECEh
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], al
add byte ptr [eax], al
add byte ptr [ecx+00h], al
push es
push eax
xchg eax, ebx
add ah, byte ptr [ecx+edi*2+72h]
imul esi, dword ptr [edx+65h], 64h

Copyright Joe Security LLC 2021

Instruction
jnc 00007F44BCECE697h
outsb
add byte ptr [edx], ch
int1
add al, byte ptr [eax]
add byte ptr [eax], al
add bh, bh
int3
xor dword ptr [eax], eax
or al, 1Ah
wait
xor al, 5Ch
push edi
mov bp, seg?
inc eax
nop
xchg byte ptr [ebp-3Dh], bl
dec edi
loope 00007F44BCECE5DFh
jl 00007F44BCECE61Fh
xchg eax, edx
and eax, dword ptr [edx]
xor esp, eax
dec esi
lodsd
push edx
and ebx, dword ptr [edx]

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x17764	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a000	0x3822	.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	0x1a8	.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	0x16d48	0x17000	False	0.439017917799	data	6.15247427314	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x18000	0x1260	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1a000	0x3822	0x4000	False	0.4619140625	data	5.13551103483	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1cf7a	0x8a8	data		
RT_ICON	0x1c8b2	0x6c8	data		
RT_ICON	0x1c34a	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1b2a2	0x10a8	data		

Copyright Joe Security LLC 2021

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1a91a	0x988	data		
RT_ICON	0x1a4b2	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1a458	0x5a	data		
RT_VERSION	0x1a1e0	0x278	data	English	United States

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaLenBstr, __vbaStrVarMove, __vbaFreeVarList, __vbaEnd, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaSetSystemError, __vbaHresultCheckObj, __vbaLenBstrB, _adj_fdiv_m32, __vbaAryDestruct, __vbaOnError, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaFpR8, __vbaVarTstLt, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaStrCmp, __vbaObjVar, DllFunctionCall, _adj_fpatan, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, __vbaStrVarVal, _CIlog, __vbaNew2, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaLateMemCall, __vbaVarAdd, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaLateMemCallLd, _CIatan, __vbaStrMove, _allmul, __vbaLateIdSt, _CItan, __vbaFPInt, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0409 0x04b0
InternalName	KOPEKER
FileVersion	1.00
CompanyName	Cluster-C
Comments	Cluster-C
ProductName	Cluster-C
ProductVersion	1.00
FileDescription	Cluster-C
OriginalFilename	KOPEKER.exe

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: KOPEKER.exe PID: 5760 Parent PID: 5856

General

Start time:	08:42:44
Start date:	19/04/2021
Path:	C:\Users\user\Desktop\KOPEKER.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KOPEKER.exe'
Imagebase:	0x400000
File size:	118784 bytes
MD5 hash:	CD885321B35B73421CD63E3150D677F7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Visual Basic
Yara matches:	• Rule: JoeSecurity_GuLoader, Description: Yara detected GuLoader, Source: 00000000.00000002.985827741.0000000000620000.00000040.00000001.sdmp, Author: Joe Security
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