ID: 395385
Sample Name: SecuriteInfo.com.Mal.Generic-S.24480.13627
Cookbook: default.jbs
Time: 13:27:41
Date: 22/04/2021
Version: 31.0.0 Emerald

Table of Contents

Analysis Report SecuriteInfo.com.Mal.Generic-S.24480….

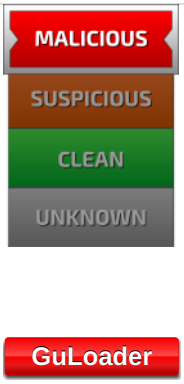
Overview

General Information

Sample Name:	SecuriteInfo.com.Mal.Generic-S.24480.13627 (renamed file extension from 13627 to exe)
Analysis ID:	395385
MD5:	fe81c0cdf996335..
SHA1:	389709fb8a2845f..
SHA256:	c4c6dc5465aa16…
Tags:	GuLoader
Infos:	

Most interesting Screenshot:

Detection

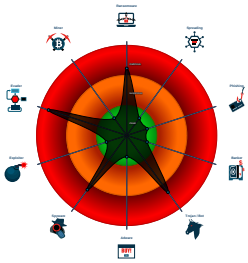


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Potential malicious icon found
- Yara detected Generic Dropper
- Yara detected GuLoader
- 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**
- SecuriteInfo.com.Mal.Generic-S.24480.exe (PID: 5948 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Mal.Generic-S.24480.exe' MD5: FE81C0CDF996335C5D5A6F75B564DA51)
  - SecuriteInfo.com.Mal.Generic-S.24480.exe (PID: 6412 cmdline: 'C:\Users\user\Desktop\SecuriteInfo.com.Mal.Generic-S.24480.exe' MD5: FE81C0CDF996335C5D5A6F75B564DA51)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

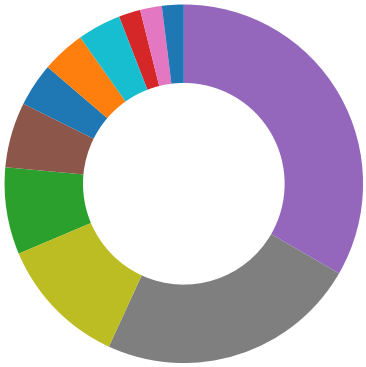
Memory Dumps

Source	Rule	Description	Author	Strings
Process Memory Space: SecuriteInfo.com.Mal.Generic-S.24480.exe PID: 5948	JoeSecurity_VB6DownloaderGeneric	Yara detected VB6 Downloader Generic	Joe Security	
Process Memory Space: SecuriteInfo.com.Mal.Generic-S.24480.exe PID: 5948	JoeSecurity_GuLoader	Yara detected GuLoader	Joe Security	
Process Memory Space: SecuriteInfo.com.Mal.Generic-S.24480.exe PID: 6412	JoeSecurity_GenericDropper	Yara detected Generic Dropper	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
- Stealing of Sensitive Information

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

System Summary:

Potential malicious icon found

Data Obfuscation:

Yara detected GuLoader

Yara detected VB6 Downloader Generic

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

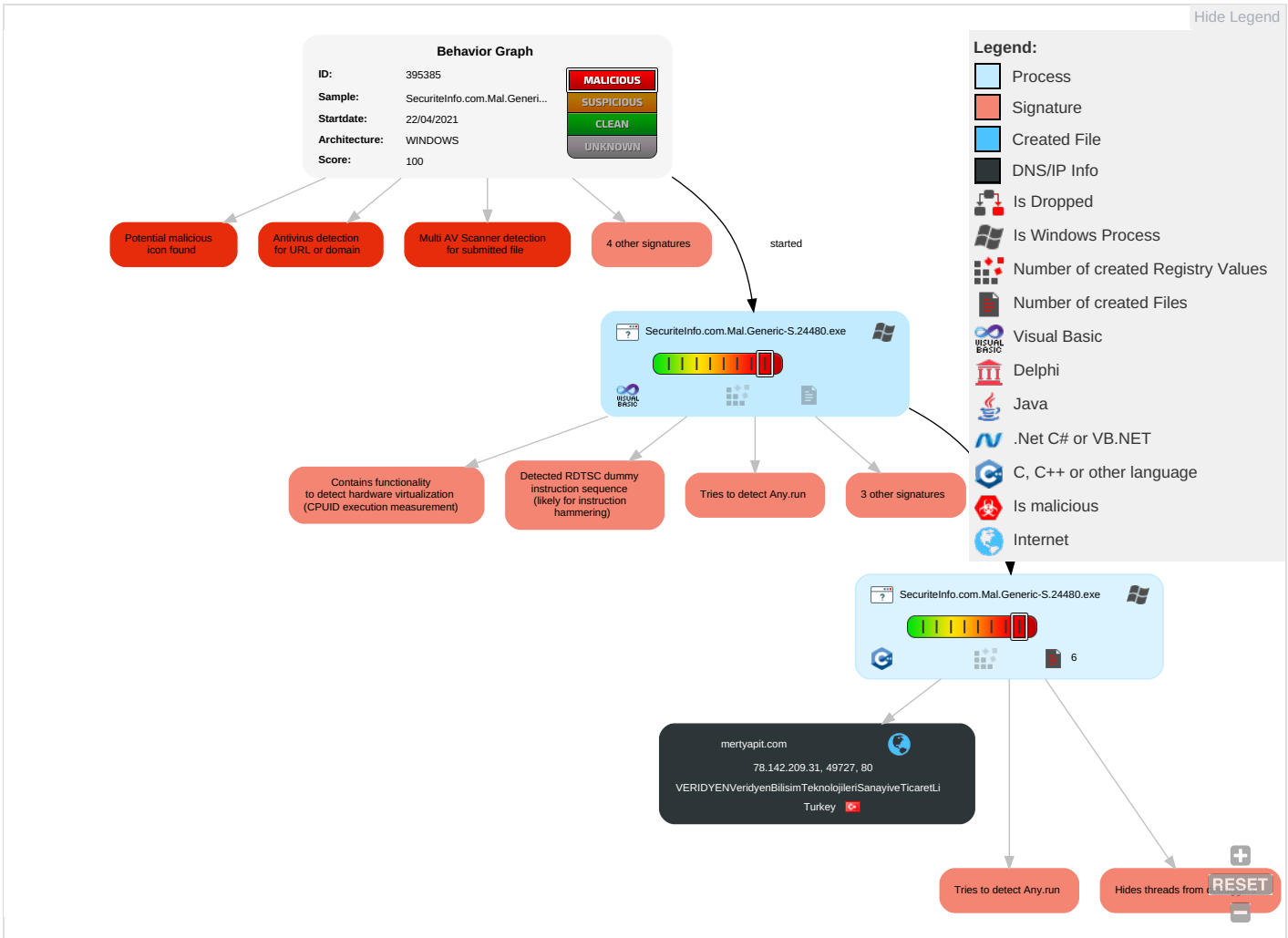
Stealing of Sensitive Information:

Yara detected Generic Dropper

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Path Interception	Process Injection 1 2	Virtualization/Sandbox Evasion 2 3	Input Capture 1	Security Software Discovery 7 2 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop or Insecure Network Communicati
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Process Injection 1 2	LSASS Memory	Virtualization/Sandbox Evasion 2 3	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 t Redirect Pho Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 t Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicati
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	System Information Discovery 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

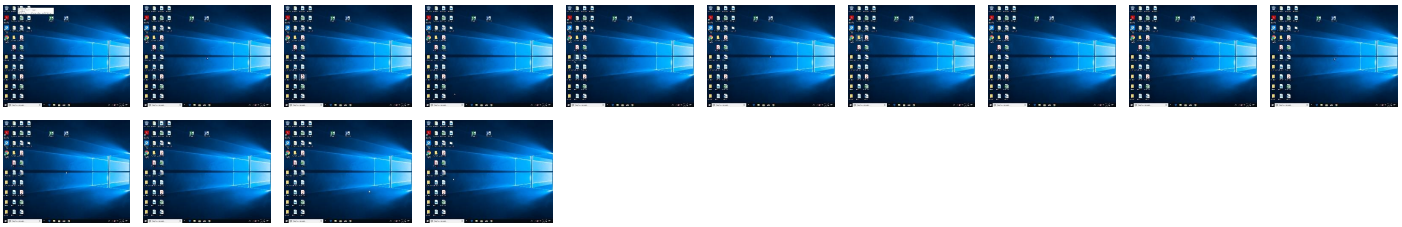
Behavior Graph



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
SecuriteInfo.com.Mal.Generic-S.24480.exe	28%	Virustotal		Browse
SecuriteInfo.com.Mal.Generic-S.24480.exe	21%	ReversingLabs	Win32.Backdoor.Remcos	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
mertyapit.com	3%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://mertyapit.com/abcd/lndb_isQxc208.bin	3%	Virustotal		Browse
http://mertyapit.com/abcd/lndb_isQxc208.bin	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mertyapit.com	78.142.209.31	true	false	• 3%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://mertyapit.com/abcd/lndb_isQxc208.bin	true	• 3%, Virustotal, Browse • Avira URL Cloud: malware	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
78.142.209.31	mertyapit.com	Turkey		209853	VERIDYENVeridyenBilisimTeknolojileriSanayiveTicaretLi	false

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	395385
Start date:	22.04.2021
Start time:	13:27:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 28s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Mal.Generic-S.24480.13627 (renamed file extension from 13627 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:	27
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.spyw.evad.winEXE@3/0@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 59.5% (good quality ratio 51.8%) • Quality average: 71.1% • Quality standard deviation: 33.2%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings:	Show All • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, UsoClient.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 20.50.102.62, 93.184.220.29, 13.88.21.125, 52.147.198.201, 92.122.145.220, 40.88.32.150, 184.30.24.56, 104.42.151.234, 13.107.42.23, 13.107.5.88, 67.27.233.126, 67.27.159.126, 67.26.83.254, 67.26.139.254, 67.27.158.254, 92.122.213.194, 92.122.213.247, 13.64.90.137, 104.43.139.144, 20.82.210.154, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, cs9.wac.phicdn.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, e12564.dspb.akamaiedge.net, skypedataprdcoleus15.cloudapp.net, ocsp.digicert.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, arc.trafficmanager.net, 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, config.edge.skype.com, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, afdo-tas-offload.trafficmanager.net, dual-a-0001.a-msedge.net, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus16.cloudapp.net, skypedataprdcoleus16.cloudapp.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, ris.api.iris.microsoft.com, a-0001.a-afdentry.net.trafficmanager.net, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, l-0014.l-msedge.net, skypedataprdcolwus15.cloudapp.net, skypedataprdcolwus16.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory 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

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
VERIDYENVeridyenBilisimTeknolojileriSanayiveTicaretLi	PowerShell_Input.ps1	Get hash	malicious	Browse	• 185.149.100.223
	Sample.doc	Get hash	malicious	Browse	• 185.149.100.223
	Sample.doc	Get hash	malicious	Browse	• 185.149.100.223
	m5bCbJdk7l.exe	Get hash	malicious	Browse	• 78.142.208.189
	Receipt 01.xlsx	Get hash	malicious	Browse	• 78.142.208.189
	P87k5f5ecn.exe	Get hash	malicious	Browse	• 78.142.208.189
	vB1Zux02Zf.exe	Get hash	malicious	Browse	• 78.142.208.189
	SecuriteInfo.com.BehavesLike.Win32.Generic.ch.exe	Get hash	malicious	Browse	• 78.142.208.9
	4vnTrjsACd.rtf	Get hash	malicious	Browse	• 78.142.208.189
	NsNu725j8o.exe	Get hash	malicious	Browse	• 78.142.208.189
	Qs6ySVV95N.exe	Get hash	malicious	Browse	• 78.142.208.189
	ugGgUEbqio.exe	Get hash	malicious	Browse	• 78.142.208.189
	Details here.exe	Get hash	malicious	Browse	• 78.142.208.9
	wkHpvThL2E.exe	Get hash	malicious	Browse	• 78.142.208.189
	415801-13-4-87946.doc	Get hash	malicious	Browse	• 45.151.250.142
	Confirm!!!..exe	Get hash	malicious	Browse	• 78.142.208.9
	wDMBDrN663.exe	Get hash	malicious	Browse	• 78.142.208.189
	http://www.rekmall.net/.well-known/acme-challenge/act_contactar2/admin_cat/mgc_chatbox/information-12/pspbrwse.php?sit=ervw1yb1atp20npd0&remember=quiet&feel=sleep	Get hash	malicious	Browse	• 45.151.250.202
	file.exe	Get hash	malicious	Browse	• 78.142.209.253
	NEW ORDER 15DEC.xlsx	Get hash	malicious	Browse	• 78.142.208.189

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):	6.119482475975053
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:	SecuriteInfo.com.Mal.Generic-S.24480.exe
File size:	156976
MD5:	fe81c0cdf996335c5d5a6f75b564da51
SHA1:	389709fb8a2845f373c82ff74f9478d11b115326

General

SHA256:	c4c6dc5465aa1676119c00c0b45c0f3be1d525e31eff1d87072952f839e5cbf9
SHA512:	bca1924b48e15f11a3160727e0b4551860bc19b7f38a573a97d4ef34670d5355201b89fff365371c4cb74a4b5af2b6e8f5c06d36a7f83b05aeda9d6b5dcc7c62
SSDEEP:	3072:I/ccO4OT8moEt1upckfHZMUJ5g1igndol9unRzZYEEFSd:I/ccO4gwsupckfHZMUJ5g1igdS9uRzZD
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...+Y.R..... ....0.....0....@.....

File Icon

Icon Hash:	20047c7c70f0e004

Static PE Info

General

Entrypoint:	0x401710
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x52B5592B [Sat Dec 21 09:02:35 2013 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:	7a3a70cb080199018e93a3de757ce707

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	E=mdregruppen@Rimper.Fl, CN=Tyvstarterne4, OU=Trizonal, O=FACITLISTERNE, L=DATTERLIG, S=Ocypodan, C=TF
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 4/21/2021 5:11:46 PM 4/21/2022 5:11:46 PM
Subject Chain	• E=mdregruppen@Rimper.Fl, CN=Tyvstarterne4, OU=Trizonal, O=FACITLISTERNE, L=DATTERLIG, S=Ocypodan, C=TF
Version:	3
Thumbprint MD5:	9AB0B51E5335FEA6F39FDF3DFED1017F
Thumbprint SHA-1:	8F755B4ED53F46B44C763BFE66186448BA0D3B87
Thumbprint SHA-256:	8E71BB6F9E36D25552FF3B1012A83650C073C6677E18EF2FAC5914739DDA3A23
Serial:	00

Entrypoint Preview

Instruction
push 00401930h
call 00007F96C08B8DD5h
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

Instruction
inc eax
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [ecx], bh
fsubr dword ptr [ecx]
jnc 00007F96C08B8E2Eh
xchg eax, ecx

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x21ba4	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x25000	0x900	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x25000	0x1530	
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	0x184	.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	0x211c0	0x22000	False	0.382044175092	data	6.31771354021	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x23000	0x12b0	0x1000	False	0.00634765625	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x25000	0x900	0x1000	False	0.166748046875	data	1.99303359091	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x257d0	0x130	data		
RT_ICON	0x254e8	0x2e8	data		
RT_ICON	0x253c0	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x25390	0x30	data		
RT_VERSION	0x25150	0x240	data	Chinese	Taiwan

Imports

DLL	Import
MSVBVM60.DLL	_CIcos, _adj_fptan, __vbaVarMove, __vbaFreeVar, __vbaAryMove, __vbaStrVarMove, __vbaEnd, __vbaFreeVarList, _adj_fdiv_m64, __vbaFreeObjList, _adj_fprem1, __vbaRecAnsiToUni, __vbaSetSystemError, __vbaRecDestruct, __vbaHresultCheckObj, _adj_fdiv_m32, __vbaAryDestruct, __vbaObjSet, _adj_fdiv_m16i, __vbaObjSetAddref, _adj_fdivr_m16i, __vbaCyStr, __vbaFpR8, _CIsin, __vbaChkstk, EVENT_SINK_AddRef, __vbaGenerateBoundsError, __vbaStrCmp, __vbaAryConstruct2, DllFunctionCall, _adj_fpatan, __vbaLateIdCallLd, __vbaRecUniToAnsi, EVENT_SINK_Release, _CIsqrt, EVENT_SINK_QueryInterface, __vbaFpCmpCy, __vbaExceptHandler, _adj_fprem, _adj_fdivr_m64, __vbaFPException, _CIlog, __vbaNew2, __vbaVar2Vec, __vbaR8Str, __vbaInStr, _adj_fdiv_m32i, _adj_fdivr_m32i, __vbaStrCopy, __vbaI4Str, __vbaFreeStrList, _adj_fdivr_m32, _adj_fdiv_r, __vbaVarTstNe, __vbaI4Var, __vbaStrToAnsi, __vbaVarDup, __vbaFpI4, __vbaRecDestructAnsi, _CIatan, __vbaStrMove, __vbaCastObj, _allmul, __vbaLateIdSt, _CItan, _CIexp, __vbaFreeStr, __vbaFreeObj

Version Infos

Description	Data
Translation	0x0404 0x04b0
InternalName	coalman

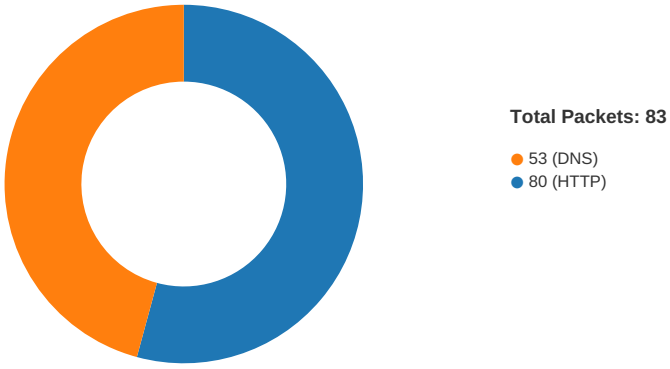
Description	Data
FileVersion	1.00
CompanyName	Green Stream Software
ProductName	Green Stream Software
ProductVersion	1.00
OriginalFilename	coalman.exe

Possible Origin

Language of compilation system	Country where language is spoken	Map
Chinese	Taiwan	

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2021 13:29:18.225480080 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.307781935 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.307885885 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.308357000 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.389518023 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.390770912 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.390805006 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.390829086 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.390861988 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.390862942 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.390882969 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.390886068 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.390904903 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.390927076 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.390934944 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.390955925 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.390983105 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.391043901 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.391067028 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.391092062 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.391108990 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472024918 CEST	80	49727	78.142.209.31	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2021 13:29:18.472070932 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472096920 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472122908 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472129107 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472146034 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472152948 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472172022 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472186089 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472197056 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472208023 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472220898 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472244024 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472249031 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472270966 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472275019 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472297907 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472300053 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472320080 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472325087 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472337008 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472348928 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472357988 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472374916 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472393036 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472399950 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472410917 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472424030 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472429037 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472454071 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.472461939 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.472496986 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.473521948 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.473625898 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553147078 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553174973 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553200006 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553222895 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553231001 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553244114 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553251982 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553265095 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553291082 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553309917 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553421021 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553447008 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553467035 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553479910 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553483009 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553505898 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553514957 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553533077 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553534985 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553556919 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553572893 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553579092 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553596973 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553600073 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553621054 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553627014 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553647995 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553673029 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553690910 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553714037 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553735018 CEST	80	49727	78.142.209.31	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2021 13:29:18.553739071 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553760052 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553777933 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553894997 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553921938 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553946018 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553950071 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553966045 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.553982973 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.553986073 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.554008961 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.554009914 CEST	49727	80	192.168.2.3	78.142.209.31
Apr 22, 2021 13:29:18.554028988 CEST	80	49727	78.142.209.31	192.168.2.3
Apr 22, 2021 13:29:18.554047108 CEST	49727	80	192.168.2.3	78.142.209.31

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2021 13:28:21.761200905 CEST	50620	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:21.775052071 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:21.818528891 CEST	53	50620	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:21.826889992 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:21.924453974 CEST	60152	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:21.973376036 CEST	53	60152	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:22.296538115 CEST	57544	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:22.348061085 CEST	53	57544	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:23.414343119 CEST	55984	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:23.463987112 CEST	53	55984	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:24.336591005 CEST	64185	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:24.388118982 CEST	53	64185	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:24.791631937 CEST	65110	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:24.850301027 CEST	53	65110	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:25.452760935 CEST	58361	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:25.503132105 CEST	53	58361	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:26.554866076 CEST	63492	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:26.603543043 CEST	53	63492	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:27.740609884 CEST	60831	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:27.797853947 CEST	53	60831	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:29.173465967 CEST	60100	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:29.224911928 CEST	53	60100	8.8.8.8	192.168.2.3
Apr 22, 2021 13:28:59.035937071 CEST	53195	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:28:59.121874094 CEST	53	53195	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:01.548304081 CEST	50141	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:01.599793911 CEST	53	50141	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:06.155900955 CEST	53023	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:06.204499960 CEST	53	53023	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:06.779205084 CEST	58722	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:06.779494047 CEST	56596	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:06.779568911 CEST	64101	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:06.828001022 CEST	53	58722	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:06.828078985 CEST	53	56596	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:06.828098059 CEST	53	64101	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:08.123630047 CEST	49563	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:08.187468052 CEST	53	49563	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:09.667340994 CEST	51352	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:09.722791910 CEST	53	51352	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:11.263891935 CEST	59349	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:11.320943117 CEST	53	59349	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:12.764857054 CEST	57084	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:12.814733982 CEST	53	57084	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:17.009279013 CEST	58823	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:17.058104038 CEST	53	58823	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:18.092855930 CEST	57568	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:18.198590994 CEST	53	57568	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 22, 2021 13:29:18.457473993 CEST	50540	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:18.506721020 CEST	53	50540	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:24.176218033 CEST	54366	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:24.225965977 CEST	53	54366	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:31.824414968 CEST	53034	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:31.889034986 CEST	53	53034	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:45.301484108 CEST	57762	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:45.352994919 CEST	53	57762	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:56.780606031 CEST	55435	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:56.830948114 CEST	53	55435	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:57.792860985 CEST	50713	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:57.841581106 CEST	53	50713	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:58.601203918 CEST	56132	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:58.652570963 CEST	53	56132	8.8.8.8	192.168.2.3
Apr 22, 2021 13:29:59.486447096 CEST	58987	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:29:59.535092115 CEST	53	58987	8.8.8.8	192.168.2.3
Apr 22, 2021 13:30:00.718856096 CEST	56579	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:30:00.772932053 CEST	60633	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:30:00.776736975 CEST	53	56579	8.8.8.8	192.168.2.3
Apr 22, 2021 13:30:00.821571112 CEST	53	60633	8.8.8.8	192.168.2.3
Apr 22, 2021 13:30:04.236038923 CEST	61292	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:30:04.297532082 CEST	53	61292	8.8.8.8	192.168.2.3
Apr 22, 2021 13:30:08.439625978 CEST	63619	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:30:08.501127958 CEST	53	63619	8.8.8.8	192.168.2.3
Apr 22, 2021 13:30:22.884633064 CEST	64938	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:30:22.952339888 CEST	53	64938	8.8.8.8	192.168.2.3
Apr 22, 2021 13:30:37.972486019 CEST	61946	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:30:38.021482944 CEST	53	61946	8.8.8.8	192.168.2.3
Apr 22, 2021 13:30:39.099416018 CEST	64910	53	192.168.2.3	8.8.8.8
Apr 22, 2021 13:30:39.165184021 CEST	53	64910	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 22, 2021 13:29:18.092855930 CEST	192.168.2.3	8.8.8.8	0x2d9c	Standard query (0)	mertyapit.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 22, 2021 13:29:18.198590994 CEST	8.8.8.8	192.168.2.3	0x2d9c	No error (0)	mertyapit.com		78.142.209.31	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- mertyapit.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49727	78.142.209.31	80	C:\Users\user\Desktop\SecuriteInfo.com.Mal.Generic-S.24480.exe

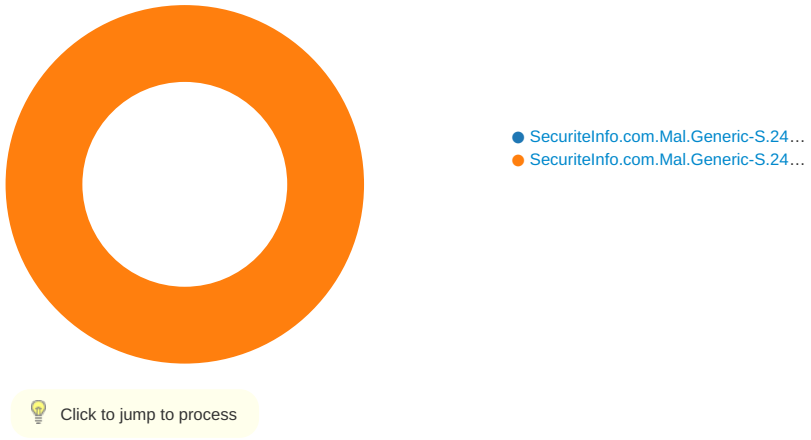
Timestamp	kBytes transferred	Direction	Data
Apr 22, 2021 13:29:18.308357000 CEST	1557	OUT	GET /abcd/lndb_isQxc208.bin HTTP/1.1 User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko Host: mertyapit.com Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Apr 22, 2021 13:29:18.390770912 CEST	1557	IN	HTTP/1.1 200 OK Connection: Keep-Alive Content-Type: application/octet-stream Last-Modified: Thu, 22 Apr 2021 00:08:57 GMT Accept-Ranges: bytes Content-Length: 164416 Date: Thu, 22 Apr 2021 11:29:17 GMT

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Mal.Generic-S.24480.exe PID: 5948 Parent PID: 5672

General

Start time:	13:28:29
Start date:	22/04/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Mal.Generic-S.24480.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Mal.Generic-S.24480.exe'
Imagebase:	0x400000
File size:	156976 bytes
MD5 hash:	FE81C0CDF996335C5D5A6F75B564DA51
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

Analysis Process: SecuriteInfo.com.Mal.Generic-S.24480.exe PID: 6412 Parent PID: 5948

General

Start time:	13:29:08
Start date:	22/04/2021
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Mal.Generic-S.24480.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\SecuriteInfo.com.Mal.Generic-S.24480.exe'
Imagebase:	0x400000
File size:	156976 bytes
MD5 hash:	FE81C0CDF996335C5D5A6F75B564DA51
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	4182A7	NtReadFile

Disassembly

Code Analysis