ID: 662065
Sample Name:
SecuriteInfo.com.Variant.Jaik.84784.3654.20731
Cookbook: default.jbs
Time: 17:42:07
Date: 12/07/2022
Version: 35.0.0 Citrine

Table of Contents

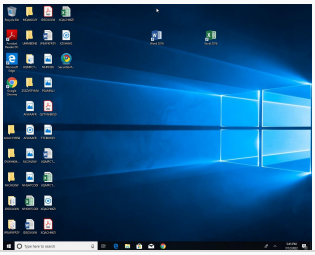
Windows Analysis Report

SecuriteInfo.com.Variant.Jaik.84784.3654.20731

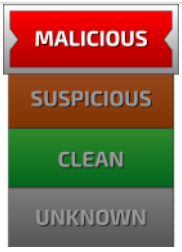
Overview

General Information

Sample Name:	SecuriteInfo.com.Variant.Jaik.84784.3654.20731 (renamed file extension from 20731 to exe)
Analysis ID:	662065
MD5:	74cd3c3d32dcf5…
SHA1:	d7ec9719a6e5ea..
SHA256:	cb943da125fde1..
Tags:	exe
Infos:	



Detection



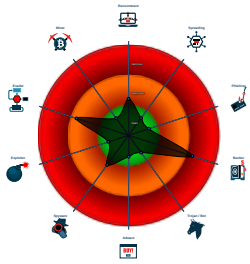
Dridex Dropper

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Antivirus detection for dropped file
- Dridex dropper found
- Machine Learning detection for sam…
- Uses 32bit PE files
- PE file contains strange resources
- Drops PE files
- Contains functionality to check if a d…
- Contains functionality to query local…
- Uses code obfuscation techniques (…
- Checks if the current process is bei…
- PE file contains sections with non-s…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Variant.Jaik.84784.3654.exe (PID: 6288 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe" MD5: 74CD3C3D32DCF5029D1BC66347F44AF7)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for dropped file

Machine Learning detection for sample

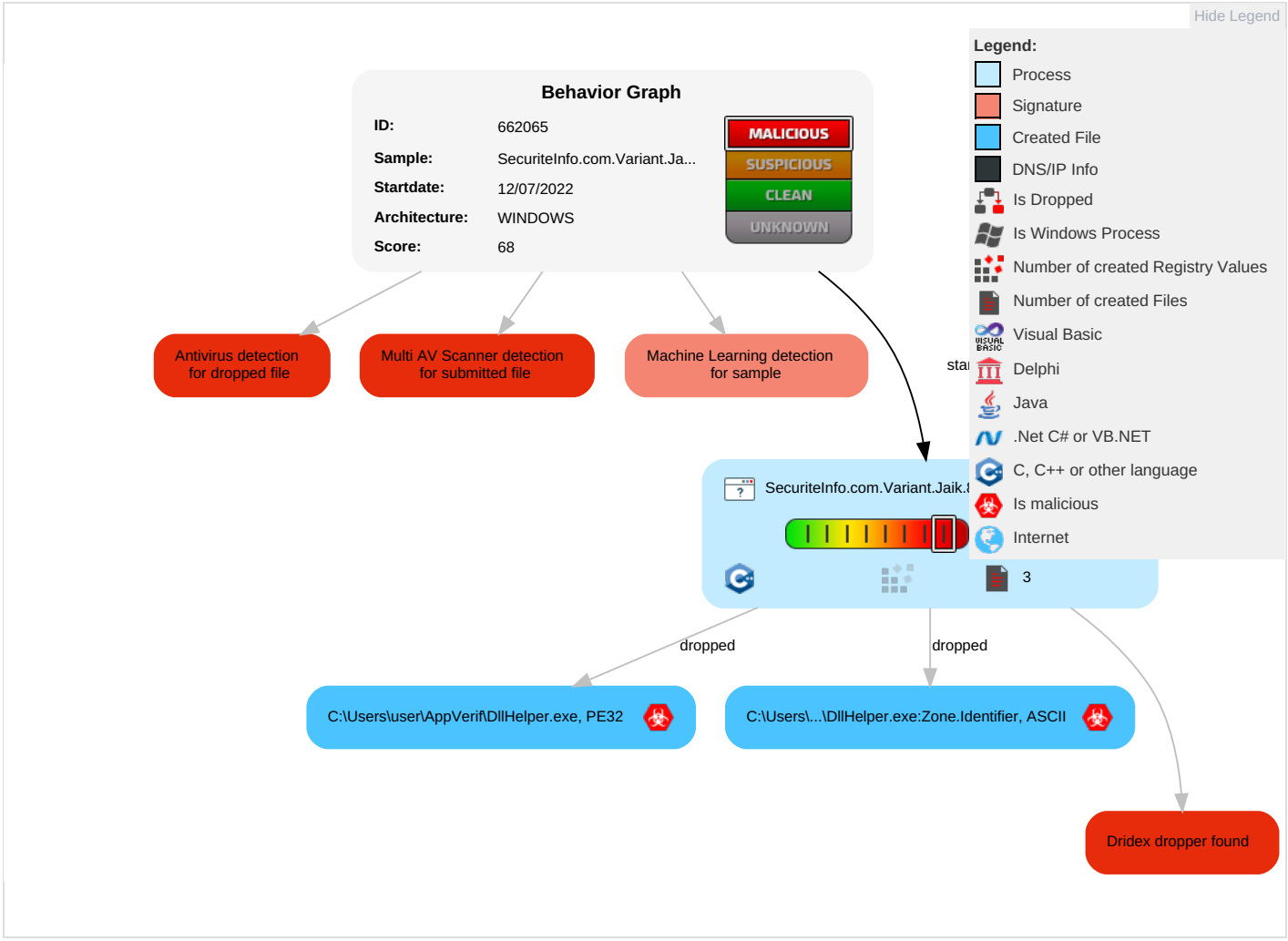
E-Banking Fraud

Dridex dropper found

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	Impact
Valid Accounts	2 Native API	Path Interception	Path Interception	1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Virtualization/Sandbox Evasion	LSASS Memory	4 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	2 Software Packing	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Deobfuscate/Decode Files or Information	NTDS	1 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	3 Obfuscated Files or Information	LSA Secrets	1 2 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

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.Variant.Jaik.84784.3654.exe	59%	Virustotal		Browse
SecuriteInfo.com.Variant.Jaik.84784.3654.exe	69%	ReversingLabs	Win32.Trojan.Jaik	
SecuriteInfo.com.Variant.Jaik.84784.3654.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppVerif\DllHelper.exe	100%	Avira	TR/Dropper.Gen7	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	662065
Start date and time: 12/07/202217:42:07	2022-07-12 17:42:07 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 13s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Variant.Jaik.84784.3654.20731 (renamed file extension from 20731 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:	16
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:	mal68.bank.winEXE@1/2@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 3.4% (good quality ratio 3.3%) • Quality average: 70.7% • Quality standard deviation: 18.5%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, store-images.s-microsoft.com-c.edgekey.net, arc.msn.com, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

Time	Type	Description
17:45:30	Task Scheduler	Run new task: COMSurrogate path: C:\Users\user\AppVerif\DllHelper.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppVerif\DllHelper.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	480444416
Entropy (8bit):	0.06514875317096143
Encrypted:	false
SSDEEP:	
MD5:	BD864AE710BD408189F12305EEDC2008
SHA1:	D6EB0CE0A3F94D8A288B0A6B50DC02DF2EE22B35
SHA-256:	CE16864816826C0D87BEC3473B15F215D7F572D8DDD52600E4C82D834F535D10
SHA-512:	049FE137771902D76BE572A069A607B1B0BD25C638DED9752B6E572758E9093ABB258F95368E1310C05175BCD4139F7901202241FBDA068074CDFB9895439A82
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...h..h..h..v...y..v...T..v.....O..k..h.....v...j..v...i..h...i..v...i..Richh... .....PE..L...,.{].....@.....@.....l...(...`.....x.....@..... .....text...`..... ..`.data...h1.....@....tenio.....P.....@....rsrc.....`.....@..@.reloc..rG.....H...0.....@..B..... ....

C:\Users\user\AppVerif\DllHelper.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621

Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.789455480828862
TrID:	• Win32 Executable (generic) a (10002005/4) 99.53% • InstallShield setup (43055/19) 0.43% • 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.Variant.Jaik.84784.3654.exe
File size:	1870760
MD5:	74cd3c3d32dcf5029d1bc66347f44af7
SHA1:	d7ec9719a6e5ea0b386ef590b1b74c317e597ff8
SHA256:	cb943da125fde19e41c965a9f260caf79a6fca98c89b83bde609b843be0da377
SHA512:	6b1340641f1f7820755ccc9e78b083ab32444d560274103e21a3ccaf4dee93b62340a6445960dc5a8f09a0de87c138e182a2c1012fdaf4f4d6d39e88922451fe
SSDEEP:	49152:yCu54sLM0OEl6bINMreuk8i09pEkJz5lAcs5PVS7fhl:yCu5OGpQefZ0vfTsfSj
TLSH:	9D851208EA509426F4F7863451F98AADA63C94D71F4845C387E4A3FA866C3D0FE3257B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....,...h...h...h...v...y...v...T...v.....O...k...h.....v...j...v...i...h...i...v...i...Richh.....PE..L..

File Icon

Icon Hash:	e0ccbcccc2f2e4cc

Static PE Info

General

Entrypoint:	0x40cdb0
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x5D280B2C [Fri Jul 12 04:23:08 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	0
File Version Major:	5
File Version Minor:	0
Subsystem Version Major:	5
Subsystem Version Minor:	0
Import Hash:	7f1ef45f5deb563bbecd8473c31a66d3

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN=R3, O=Let's Encrypt, C=US
Signature Validation Error:	**A certificate chain could not be built to a trusted root authority**
Error Number:	-2146762486
Not Before, Not After	• 5/23/2022 2:32:40 AM 8/21/2022 2:32:39 AM
Subject Chain	• CN=www.artweaver.de
Version:	3
Thumbprint MD5:	BC879E2879685CBEB888E5D32DD8189D
Thumbprint SHA-1:	01B29404E8E3D0019404677B8E9699DF9750B294
Thumbprint SHA-256:	0FA3497022A3B9B10A0B786533C315048B785CDFE262198828BDCAB722017FC9
Serial:	03BB38E009072B417BF8459D28B7B3D18D33

Entrypoint Preview

Instruction
mov edi, edi
push ebp
mov ebp, esp
call 00007F3584C45E4Bh
call 00007F3584C3D496h
pop ebp
ret
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov edi, edi
push ebp
mov ebp, esp
push FFFFFFFEh
push 0059F440h
push 004112B0h
mov eax, dword ptr fs:[00000000h]
push eax
add esp, FFFFFF94h
push ebx
push esi
push edi
mov eax, dword ptr [005A1338h]
xor dword ptr [ebp-08h], eax
xor eax, ebp
push eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
mov dword ptr [ebp-18h], esp
mov dword ptr [ebp-70h], 00000000h
mov dword ptr [ebp-04h], 00000000h
lea eax, dword ptr [ebp-60h]
push eax
call dword ptr [004010C4h]

Instruction
mov dword ptr [ebp-04h], FFFFFFFEh
jmp 00007F3584C3D4A8h
mov eax, 00000001h
ret
mov esp, dword ptr [ebp-18h]
mov dword ptr [ebp-78h], 000000FFh
mov dword ptr [ebp-04h], FFFFFFFEh
mov eax, dword ptr [ebp-78h]
jmp 00007F3584C3D5D7h
mov dword ptr [ebp-04h], FFFFFFFEh
call 00007F3584C3D614h
mov dword ptr [ebp-6Ch], eax
push 00000001h
call 00007F3584C4738Ah
add esp, 04h
test eax, eax
jne 00007F3584C3D48Ch
push 0000001Ch
call 00007F3584C3D5CCh
add esp, 04h
call 00007F3584C450D4h
test eax, eax
jne 00007F3584C3D48Ch
push 00000010h

Rich Headers

Programming Language:	• [ASM] VS2008 build 21022 • [C++] VS2008 build 21022 • [C] VS2008 build 21022 • [IMP] VS2005 build 50727 • [RES] VS2008 build 21022 • [LNK] VS2008 build 21022

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x19fc6c	0x28	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x1a6000	0x21cc8	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x1c7800	0x13a8	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x1c8000	0x19c0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1200	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x82a8	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1bc	.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	0x19f660	0x19f800	False	0.8492162821525271	data	7.816031131002002	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x1a1000	0x3168	0x1400	False	0.3314453125	data	3.4095039121071826	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.tenio	0x1a5000	0x4	0x200	False	0.02734375	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x1a6000	0x21cc8	0x21e00	False	0.8149792435424354	data	7.4602970996808775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x1c8000	0x4772	0x4800	False	0.3001844618055556	data	3.257312610228726	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x1a6360	0x1608e	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0x1bc3f0	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16384, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1c0618	0x25a8	dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 16777216, next used block 0		
RT_ICON	0x1c2bc0	0xea8	data		
RT_ICON	0x1c3a68	0x668	data		
RT_ICON	0x1c40d0	0x10a8	dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 0, next used block 0		
RT_ICON	0x1c5178	0x8a8	dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 12707524, next used block 13232843		
RT_ICON	0x1c5a20	0x2e8	dBase IV DBT of @.DBF, block length 512, next free block index 40, next free block 2866470365, next used block 64682		
RT_ICON	0x1c5d08	0x988	data		
RT_ICON	0x1c6690	0x6c8	data		
RT_ICON	0x1c6d58	0x1e8	data		
RT_ICON	0x1c6f40	0x468	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1c73a8	0x568	GLS_BINARY_LSB_FIRST		
RT_ICON	0x1c7910	0x128	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0x1c7a38	0xca	data		
RT_VERSION	0x1c7b08	0x1bc	data		

Imports

DLL	Import
KERNEL32.dll	ExitProcess, GetCommandLineW, SearchPathW, FindVolumeClose, CreateFiber, FreeResource, CreateFileTransactedW, LoadResource, InitializeSListHead, HeapFree, MoveFileWithProgressA, GetModuleHandleW, GetCommConfig, GenerateConsoleCtrlEvent, GetProcessHeap, ClearCommBreak, SetCommTimeouts, LoadLibraryW, SwitchToFiber, GetCalendarInfoW, SetConsoleCursorPosition, GetACP, SetThreadPriority, VerifyVersionInfoW, DeleteFiber, GetLastError, SetLastError, GetProcAddress, GetProcessHeaps, SetConsoleCtrlHandler, SetFileApisToANSI, FoldStringA, GetThreadPriority, DebugSetProcessKillOnExit, WaitCommEvent, EnumSystemGeoID, CloseHandle, MoveFileTransactedW, FindActCtxSectionStringW, ResetWriteWatch, CreateThread, InterlockedIncrement, InterlockedDecrement, Sleep, InitializeCriticalSection, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, GetFullPathNameA, GetStartupInfoW, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetModuleFileNameW, HeapValidate, IsBadReadPtr, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, IsDebuggerPresent, GetDriveTypeA, GetOEMCP, GetCPInfo, IsValidCodePage, TlsGetValue, TlsAlloc, TlsSetValue, GetCurrentThreadId, TlsFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, FreeEnvironmentStringsW, GetEnvironmentStringsW, SetHandleCount, GetStdHandle, GetFileType, GetStartupInfoA, HeapDestroy, HeapCreate, VirtualFree, GetModuleFileNameA, WriteFile, FlushFileBuffers, WideCharToMultiByte, GetConsoleCP, GetConsoleMode, DebugBreak, OutputDebugStringA, WriteConsoleW, OutputDebugStringW, HeapAlloc, HeapSize, HeapReAlloc, VirtualAlloc, InitializeCriticalSectionAndSpinCount, GetCurrentDirectoryA, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, LoadLibraryA, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, SetFilePointer, CreateFileA

Network Behavior

No network behavior found

Statistics

No statistics

System Behavior

Analysis Process: SecuriteInfo.com.Variant.Jaik.84784.3654.exe PID: 6288, Parent PID: 5684

General

Target ID:	0
Start time:	17:43:18
Start date:	12/07/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Variant.Jaik.84784.3654.exe"
Imagebase:	0xb70000
File size:	1870760 bytes
MD5 hash:	74CD3C3D32DCF5029D1BC66347F44AF7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppVerif	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	356F58B	CreateDirectoryW
C:\Users\user\AppVerif\DllHelper.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	356F885	CopyFileW
C:\Users\user\AppVerif\DllHelper.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	356F885	CopyFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppVerif\DllHelper.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 2c fd fd fd 68 54 fd 68 54 fd 68 54 fd 76 fd 01 fd 79 54 fd 76 fd 10 fd 54 54 fd 76 fd 17 fd 1e 54 fd 4f 1b fd 6b 54 fd 68 55 fd 17 54 fd 76 fd 1e fd 6a 54 fd 76 fd 00 fd 69 54 fd 68 fd 03 fd 69 54 fd 76 fd 05 fd 69 54 fd 52 69 63 68 68 54 fd 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 50 45 00 00 4c 01 05	MZ@!L!This program cannot be run in DOS mode.$,hhhvyvTvOkhvj vihiviRichhPEL	success or wait	8	356F885	CopyFileW
C:\Users\user\AppVerif\DllHelper.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	356F885	CopyFileW
C:\Users\user\AppVerif\DllHelper.exe	1870760	2048	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00		success or wait	99991	356C42D	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

⊘ **No disassembly**