

JOeSandbox Cloud BASIC



ID: 596169

Sample Name:

Confirming#000092002.exe

Cookbook: default.jbs

Time: 12:33:12

Date: 24/03/2022

Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents	2
Windows Analysis Report Confirming#000092002.exe	3
Overview	3
General Information	3
Detection	3
Signatures	3
Classification	3
Process Tree	3
Malware Configuration	3
Yara Signatures	3
Sigma Signatures	3
Joe Sandbox Signatures	3
AV Detection	4
Mitre Att&ck Matrix	4
Behavior Graph	4
Screenshots	5
Thumbnails	5
Antivirus, Machine Learning and Genetic Malware Detection	5
Initial Sample	5
Dropped Files	6
Unpacked PE Files	6
Domains	6
URLs	6
Domains and IPs	6
Contacted Domains	6
World Map of Contacted IPs	6
General Information	6
Warnings	7
Simulations	7
Behavior and APIs	7
Joe Sandbox View / Context	7
IPs	7
Domains	7
ASNs	7
JA3 Fingerprints	7
Dropped Files	7
Created / dropped Files	7
Static File Info	8
General	8
File Icon	8
Static PE Info	8
General	8
Entrypoint Preview	8
Data Directories	10
Sections	10
Resources	10
Imports	10
Version Infos	11
Possible Origin	11
Network Behavior	11
Statistics	11
System Behavior	11
Analysis Process: Confirming#000092002.exePID: 6540, Parent PID: 2372	12
General	12
Disassembly	12

Windows Analysis Report

Confirming#000092002.exe

Overview

General Information

Sample Name:

Confirming#000092002.exe

Analysis ID:

596169

MD5:

24a097b3cd1e77..

SHA1:

f856350b37fae02..

SHA256:

23cae5cce339ef...

Tags:

exe

limerat

warzonerat

Infos:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score:

48

Range:

0 - 100

Whitelisted:

false

Confidence:

100%

Signatures

Multi AV Scanner detection for subm...

Uses 32bit PE files

Antivirus or Machine Learning detec...

Sample file is different than original ...

Contains functionality to check if a d...

Contains functionality to read the PE...

Uses code obfuscation techniques (...)

Detected potential crypto function

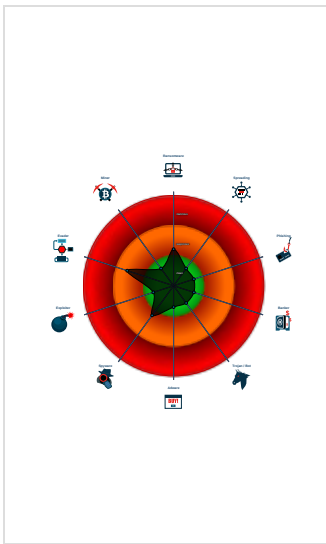
Contains functionality to create guar...

Contains functionality to query CPU...

Found potential string decryption / a...

Found large amount of non-executed...

Classification



Process Tree

System is w10x64

Confirming#000092002.exe (PID: 6540 cmdline: "C:\Users\user\Desktop\Confirming#000092002.exe" MD5: 24A097B3CD1E774E29E6E3E4F5E6522A)

cleanup

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Joe Sandbox Signatures

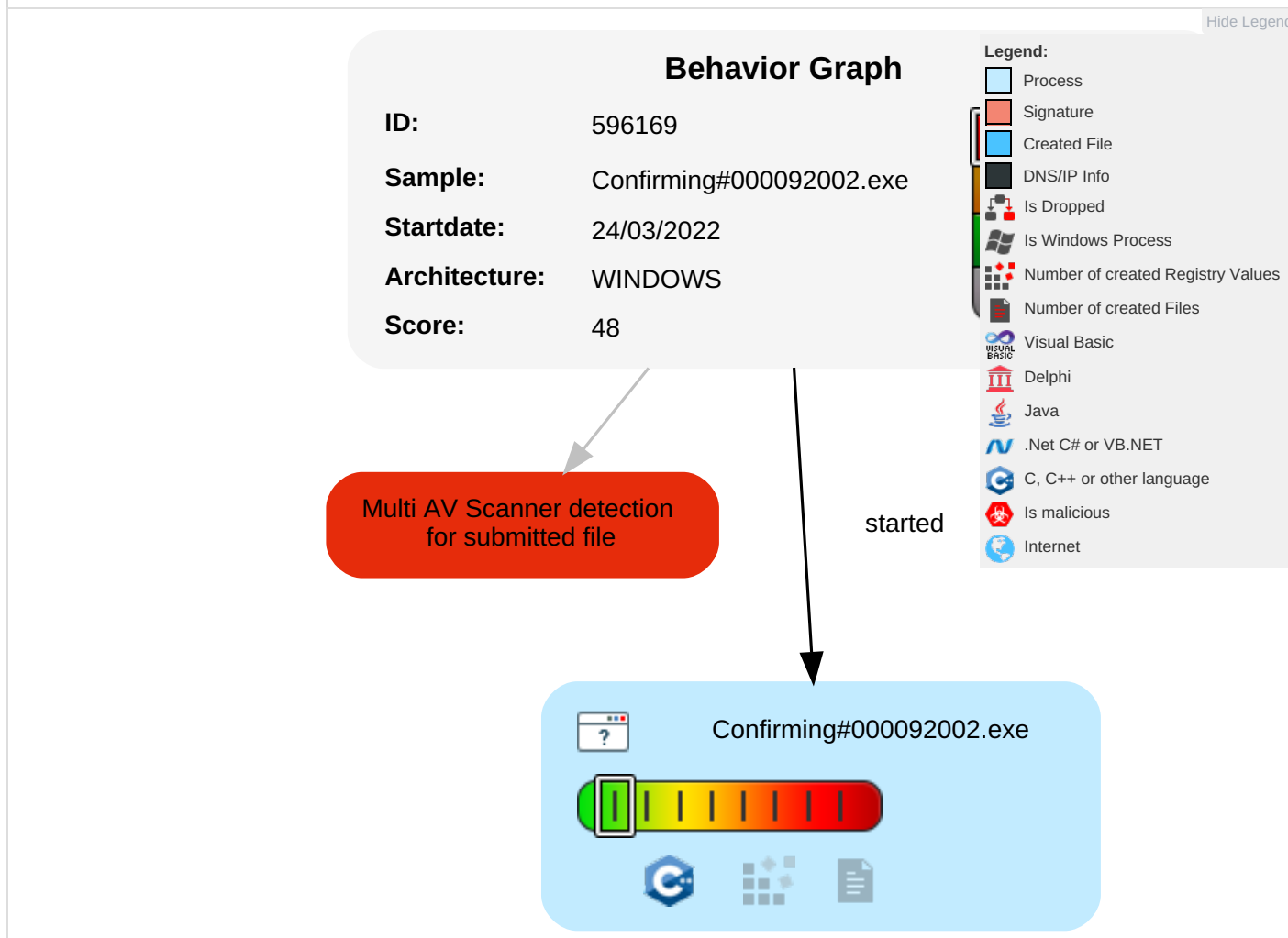


Multi AV Scanner detection for submitted file

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	Windows Management Instrumentation	Path Interception	Path Interception	1 Disable or Modify Tools	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 Software Packing	LSASS Memory	2 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)	1 Deobfuscate/Decode Files or Information	Security Account Manager	1 File and Directory Discovery	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)	2 Obfuscated Files or Information	NTDS	1 3 System Information Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud

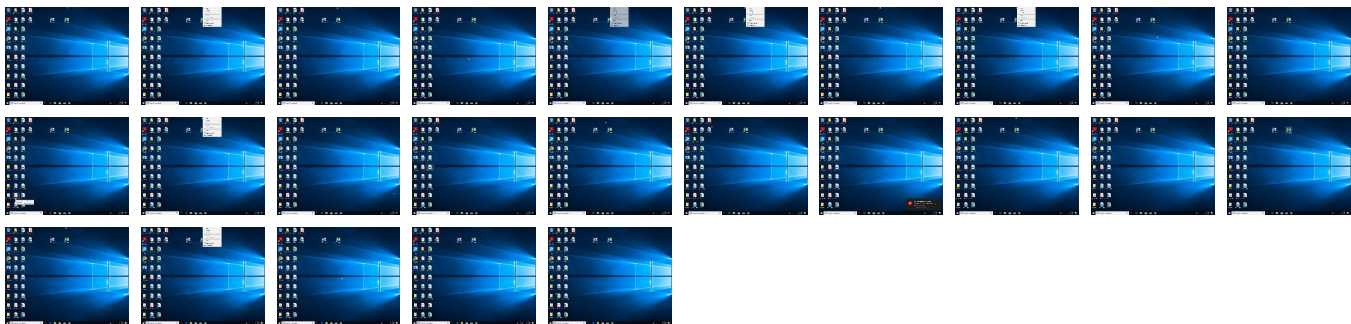
Behavior Graph



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
--------	-----------	---------	-------	------

Source	Detection	Scanner	Label	Link
Confirming#000092002.exe	55%	ReversingLabs	Win32.Trojan.Tnega	

Dropped Files

 No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.2.Confirming#000092002.exe.ea0000.0.unpack	100%	Avira	ADWARE/Adware.Gen8		Download File
1.0.Confirming#000092002.exe.ea0000.0.unpack	100%	Avira	ADWARE/Adware.Gen8		Download File

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:	34.0.0 Boulder Opal
Analysis ID:	596169
Start date and time:	2022-03-24 11:33:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 48s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Confirming#000092002.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:	mal48.winEXE@1/0@0/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 100% (good quality ratio 91.9%) • Quality average: 77.4% • Quality standard deviation: 31.2%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
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

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded domains from analysis (whitelisted): fs.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateThreadEx calls found.
- Report size getting too big, too many NtResumeThread calls found.
- Report size getting too big, too many NtTerminateThread calls found.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

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):	2.7481336301363
TrID:	- Win32 Executable (generic) a (10002005/4) 99.96% - 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:	Confirming#000092002.exe
File size:	1320960
MD5:	24a097b3cd1e774e29e6e3e4f5e6522a
SHA1:	f856350b37fae02331ce184b1f258f80900d8de5
SHA256:	23cae5cce339ef9de5d22c2117af79d45013d65241fbe6faa7a36e94e191b42b
SHA512:	bece11031bd79539c0669a62f3945d43ce0d78d768d242762c81213f471af17dc7a33c04527f1276edb27510334f8aae7b19b2cc2c204af2d560f0612e2f8651
SSDEEP:	6144:aNk8vti3OqUP1bL00RiTWSltgxCKYPMXq9NmiQBYGhpX8x4MWy1FYCz8hJ2n3C+e:Ak8l4D4pa7+ocZ
File Content Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode....\$.....V-.. ..=C..=C..=C..V@..=C..VF..=C.pEG..=C.pE@..=C.pEF.#=C..VE..=C..VG..=C..VB..=C..=B..=C..DJ..=C..D...=C..=...=C..DA..=C.Rich.=C

File Icon

	
Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x404718
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6237B381 [Sun Mar 20 23:06:41 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	5ed77736e49da7d22b203d8d8f918a6b

Entrypoint Preview

Instruction
call 00007F006871E223h
jmp 00007F006871DB8Fh
retn 0000h
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3

Instruction
int3
push 00405570h
push dword ptr fs:[00000000h]
mov eax, dword ptr [esp+10h]
mov dword ptr [esp+10h], ebp
lea ebp, dword ptr [esp+10h]
sub esp, eax
push ebx
push esi
push edi
mov eax, dword ptr [00419008h]
xor dword ptr [ebp-04h], eax
xor eax, ebp
push eax
mov dword ptr [ebp-18h], esp
push dword ptr [ebp-08h]
mov eax, dword ptr [ebp-04h]
mov dword ptr [ebp-04h], FFFFFFFEh
mov dword ptr [ebp-08h], eax
lea eax, dword ptr [ebp-10h]
mov dword ptr fs:[00000000h], eax
ret
push ebp
mov ebp, esp
and dword ptr [00542724h], 00000000h
sub esp, 24h
or dword ptr [00419010h], 01h
push 0000000Ah
call dword ptr [0041122Ch]
test eax, eax
je 00007F006871DEC2h
and dword ptr [ebp-10h], 00000000h
xor eax, eax
push ebx
push esi
push edi
xor ecx, ecx
lea edi, dword ptr [ebp-24h]
push ebx
cpuid
mov esi, ebx
pop ebx
nop
mov dword ptr [edi], eax
mov dword ptr [edi+04h], esi
mov dword ptr [edi+08h], ecx
xor ecx, ecx
mov dword ptr [edi+0Ch], edx
mov eax, dword ptr [ebp-24h]
mov edi, dword ptr [ebp-20h]
mov dword ptr [ebp-0Ch], eax
xor edi, 756E6547h
mov eax, dword ptr [ebp-18h]
xor eax, 49656E69h
mov dword ptr [ebp-04h], eax
mov eax, dword ptr [ebp-1Ch]
xor eax, 6C65746Eh
mov dword ptr [ebp-08h], eax

Data Directories			
Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x174a0	0x78	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x143000	0xd28	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x144000	0x12dc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x16380	0x54	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x162c0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x11000	0x278	.rdata
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	0xf9cd	0xfa00	False	0.605875	data	6.61019563742	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x11000	0x7322	0x7400	False	0.416386045259	data	4.90923942869	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x19000	0x129e78	0x129400	False	0.133981253942	data	2.29316435389	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x143000	0xd28	0xe00	False	0.339006696429	data	3.85073462575	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x144000	0x12dc	0x1400	False	0.7365234375	data	6.39751442919	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources					
Name	RVA	Size	Type	Language	Country
REGISTRY	0x1434d0	0xaa	ASCII text	English	United States
TYPELIB	0x1436a0	0x4d0	data	English	United States
RT_DIALOG	0x143580	0x11a	data	English	United States
RT_STRING	0x143b70	0x32	data	English	United States
RT_VERSION	0x1431f0	0x2dc	data	English	United States
RT_MANIFEST	0x143ba8	0x17d	XML 1.0 document text	English	United States

Imports	
DLL	Import

DLL	Import
KERNEL32.dll	DecodePointer, DeleteCriticalSection, GetTickCount, AcquireSRWLockExclusive, AssignProcessToJobObject, CompareStringW, ConnectNamedPipe, CreateDirectoryW, CreateEventW, CreateFileMappingW, CreateFileW, CreateloCompletionPort, CreateJobObjectW, CreateMutexW, CreateNamedPipeW, CreateProcessW, CreateRemoteThread, CreateSemaphoreW, DebugBreak, DeleteFileW, DisconnectNamedPipe, DuplicateHandle, EncodePointer, EnterCriticalSection, EnumSystemLocalesEx, EnumSystemLocalesW, ExitProcess, ExpandEnvironmentStringsW, FileTimeToSystemTime, FindClose, FindFirstFileExW, FindNextFileW, FlushFileBuffers, FlushViewOfFile, FormatMessageA, FreeEnvironmentStringsW, FreeLibrary, GetACP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetComputerNameExW, GetConsoleCP, GetConsoleMode, GetCurrentDirectoryW, GetCurrentProcess, GetCurrentProcessId, GetCurrentThread, GetDateFormatW, GetDriveTypeW, GetEnvironmentStringsW, GetExitCodeProcess, GetFileAttributesW, GetFileInformationByHandle, GetFileInformationByHandleEx, GetFileSizeEx, GetFileType, GetFullPathNameW, GetLocalTime, GetLocaleInfoW, GetLongPathNameW, CreateThread, GetModuleHandleA, GetModuleHandleExW, GetModuleHandleW, GetNativeSystemInfo, GetOEMCP, GetProcAddress, GetProcessHandleCount, GetProcessHeaps, GetProcessId, GetProcessTimes, GetQueuedCompletionStatus, GetStartupInfoW, GetStdHandle, GetStringTypeW, GetSystemDefaultLCID, GetSystemDirectoryW, GetSystemInfo, GetSystemTimeAsFileTime, GetTempPathW, GetThreadContext, GetThreadId, GetThreadLocale, GetThreadPriority, GetTimeFormatW, GetTimeZoneInformation, GetUserDefaultLCID, GetUserDefaultLangID, GetUserDefaultLocaleName, GetModuleFileNameA, SizeofResource, VirtualProtect, SetLastError, VirtualAlloc, LoadLibraryExA, LeaveCriticalSection, FindResourceA, Sleep, IsDBCSLeadByte, LoadResource, WideCharToMultiByte, lstrcpmA, GetConsoleOutputCP, SetFilePointerEx, SetStdHandle, IsValidCodePage, HeapReAlloc, HeapSize, LCMapStringW, WriteFile, VirtualQuery, LoadLibraryExW, TlsFree, TlsSetValue, TlsGetValue, TlsAlloc, InitializeCriticalSectionAndSpinCount, RaiseException, CloseHandle, GetLastError, MultiByteToWideChar, GetCurrentThreadId, InitializeCriticalSectionEx, GetModuleFileNameW, RtlUnwind, QueryPerformanceCounter, TerminateProcess, SetUnhandledExceptionFilter, UnhandledExceptionFilter, IsProcessorFeaturePresent, InitializeSListHead, GetProcessHeap, HeapFree, IsDebuggerPresent, OutputDebugStringW, HeapAlloc, WriteConsoleW
USER32.dll	CharNextA, MessageBoxA
ADVAPI32.dll	RegQueryInfoKeyW, RegDeleteKeyA, RegCreateKeyExA, RegSetValueExA, RegOpenKeyExA, RegDeleteValueA, RegEnumKeyExA, RegCloseKey
ole32.dll	CoCreateInstance, CoTaskMemFree, CoTaskMemRealloc, CoTaskMemAlloc
OLEAUT32.dll	VarUI4FromStr

Version Infos	
Description	Data
LegalCopyright	Microsoft Corporation. All rights reserved.
InternalName	MultiRead
FileVersion	1, 0, 0, 1
ProductName	MultiRead Module
ProductVersion	1, 0, 0, 1
FileDescription	MultiRead Module
OriginalFilename	MultiRead.EXE
Translation	0x0409 0x04b0

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

Network Behavior	
 No network behavior found	

Statistics	
 No statistics	

System Behavior	
-----------------	--

General

Target ID:	1
Start time:	12:34:20
Start date:	24/03/2022
Path:	C:\Users\user\Desktop\Confirming#000092002.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Confirming#000092002.exe"
Imagebase:	0xea0000
File size:	1320960 bytes
MD5 hash:	24A097B3CD1E774E29E6E3E4F5E6522A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly No disassembly