ID: 877002
Sample Name: 09212399.exe
Cookbook: default.jbs
Time: 10:49:05
Date: 28/05/2023
Version: 37.1.0 Beryl

Table of Contents

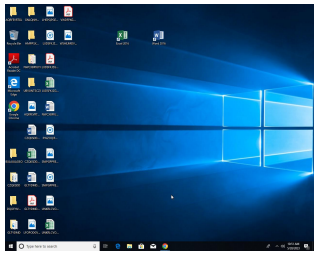
Windows Analysis Report

09212399.exe

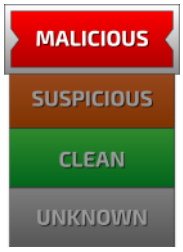
Overview

General Information

Sample Name:	09212399.exe
Analysis ID:	877002
MD5:	57dd320eae0fa..
SHA1:	fc2ce4b86d640..
SHA256:	4a524e63c81e…
Infos:	



Detection

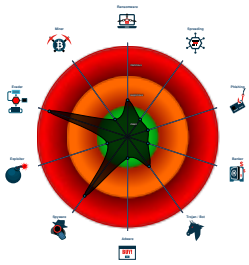


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Detected unpacking (overwrites its o…
- Yara detected AntiVM3
- Detected unpacking (changes PE se…
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Tries to harvest and steal Bitcoin W…
- Deletes itself after installation
- Tries to harvest and steal browser in…

Classification



Process Tree

- **System is w10x64**
- 09212399.exe (PID: 4968 cmdline: C:\Users\user\Desktop\09212399.exe MD5: 57DD320EAE0FADD155619407C8B5313C)
  - certreq.exe (PID: 7032 cmdline: C:\Windows\system32\certreq.exe MD5: 5A4F8BBCD943BC543B3F664C7DA83827)
    - conhost.exe (PID: 7064 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - WerFault.exe (PID: 3332 cmdline: C:\Windows\SysWOW64\WerFault.exe -u -p 4968 -s 880 MD5: 9E2B8ACAD48ECCA55C0230D63623661B)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000003.364029125.0000000002632000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.381636049.00000000023D0000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Smokeloader_3687686f	unknown	unknown	• 0x30d:$a: 0C 8B 45 F0 89 45 C8 8B 45 C8 8B 40 3C 8B 4D F0 8D 44 01 04 89
Process Memory Space: 09212399.exe PID: 4968	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

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

Machine Learning detection for sample

Compliance

Detected unpacking (overwrites its own PE header)

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Hooking and other Techniques for Hiding and Protection

Deletes itself after installation

Malware Analysis System Evasion

Yara detected AntiVM3

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

Stealing of Sensitive Information

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

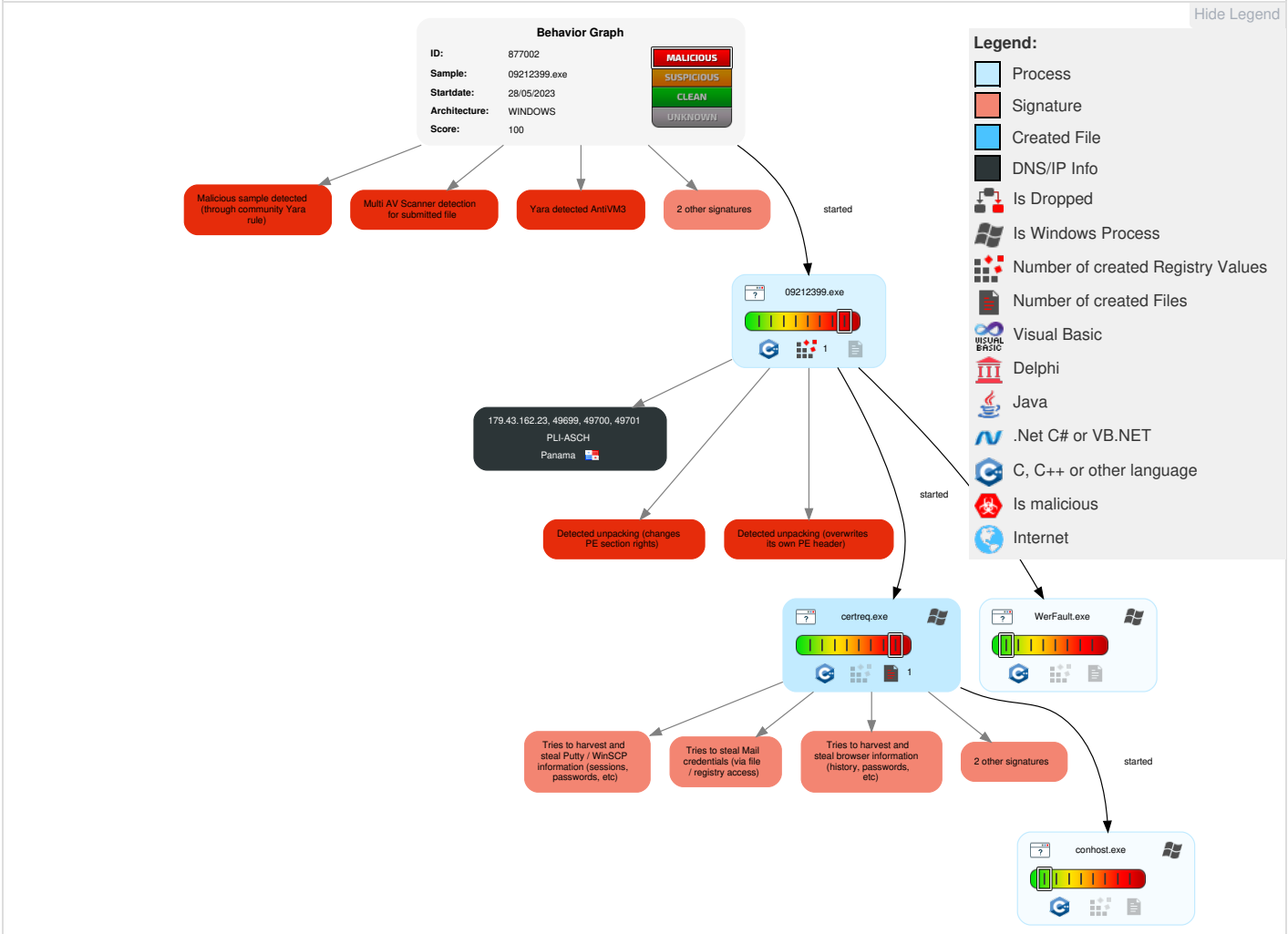
Tries to harvest and steal Bitcoin Wallet information

Tries to harvest and steal browser information (history, passwords, etc)

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	1 1 Windows Management Instrumentation	Path Interception	1 1 Process Injection	1 Virtualization/Sandbox Evasion	1 OS Credential Dumping	1 System Time Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	2 Command and Scripting Interpreter	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Credentials in Registry	1 3 1 Security Software Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Native API	Logon Script (Windows)	Logon Script (Windows)	2 Obfuscated Files or Information	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	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 2 Software Packing	NTDS	1 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	1 File Deletion	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Steganography	Cached Domain Credentials	4 7 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features

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
09212399.exe	41%	Virustotal		Browse
09212399.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://discord.com	0%	URL Reputation	safe	
http://https://discord.com	0%	URL Reputation	safe	
http://https:///etc/puk.keyGET13ConnectionupgradeUpgradewebsocketUser-AgentAccept-Encodinggzip	0%	Avira URL Cloud	safe	
http://https:///etc/puk.keyMachineGuid	0%	Avira URL Cloud	safe	
http://https://179.43.162.23:8509/c29db42cd4cdbbd4077/favicon.pngkernelbasentdllkernel32GetProcessMitigatio	0%	Avira URL Cloud	safe	
http://https://179.43.162.23:8509/c29db42cd4cdbbd4077/favicon.pngH	0%	Avira URL Cloud	safe	
http://https://179.43.162.23:8509/c29db42cd4cdbbd4077/favicon.png	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

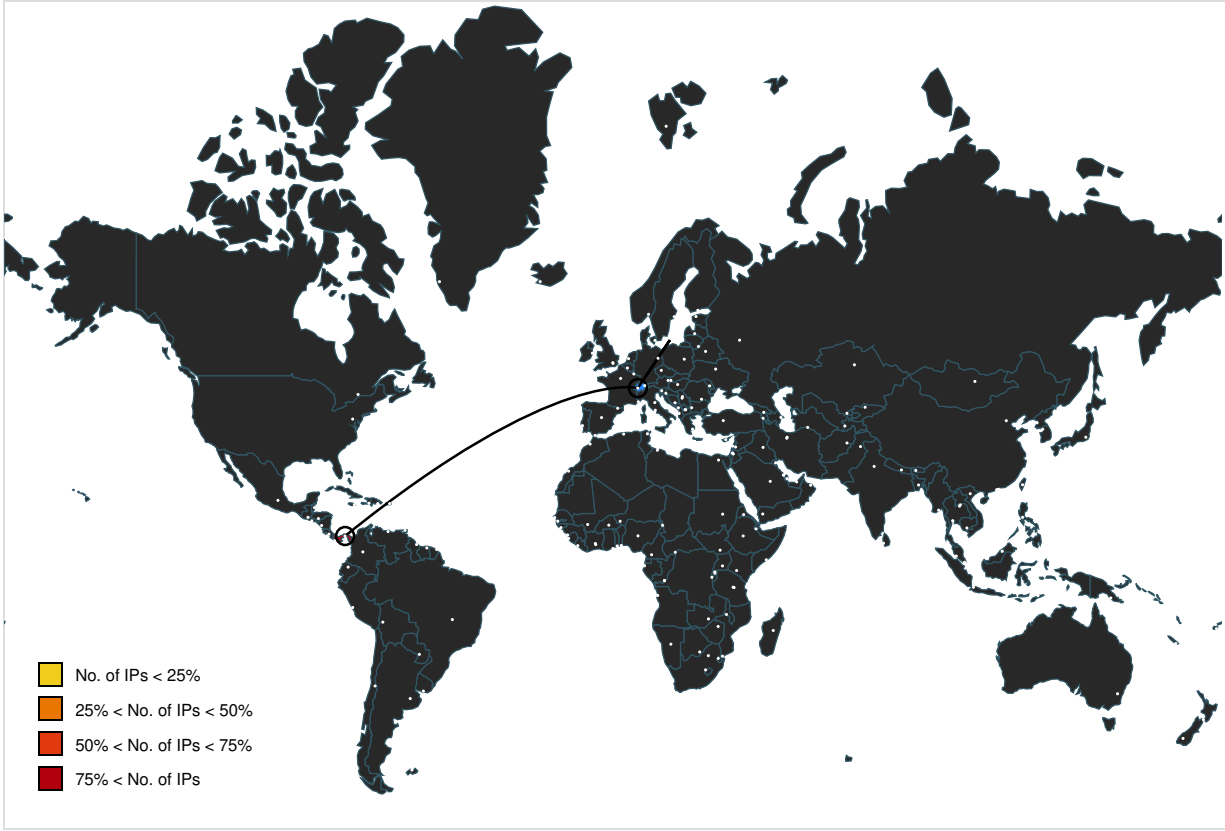
No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://discord.com	certreq.exe, 00000001.00000003.426281539.0000018823E92000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe • URL Reputation: safe	unknown
http://https://179.43.162.23:8509/c29db42cd4cdbbd4077/favicon.png	09212399.exe, 00000000.00000002.381262694.00000000000A1000.00000004.00000010.00020000.00000000.sdmp, 09212399.exe, 00000000.00000003.368127426.0000000002635000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https:///etc/puk.keyMachineGuid	certreq.exe, 00000001.00000003.413436249.0000018823DBA000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.415230877.0000018823DBF000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://179.43.162.23:8509/c29db42cd4cdbbd4077/favicon.pngkernelbasentdllkernel32GetProcessMitigatio	09212399.exe, 00000000.00000003.368127426.0000000002635000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http:// https:///etc/puk.keyGET13ConnectionupgradeUpgradewebsocketUser-AgentAccept-Encodinggzip	certreq.exe, 00000001.00000003.450923361.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.444650267.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.423142442.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.443304465.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.445666271.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.424137500.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.443537430.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.428558621.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.420232422.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.443833228.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.424761572.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.423901851.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.423640005.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.441677024.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.438459075.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.415743888.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.424370962.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.415743888.0000018823DB1000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.419657256.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.444175695.0000018823E92000.00000004.00000020.00020000.00000000.sdmp, certreq.exe, 00000001.00000003.426281539.0000018823E92000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://https://discordapp.com	certreq.exe, 00000001.00000003.426281539.0000018823E92000.00000004.00000020.00020000.00000000.sdmp	false		high
http:// https://179.43.162.23:8509/c29db42cd4cdbbd4077/favicon.pngH	09212399.exe, 00000000.00000002.381262694.00000000000A1000.00000004.00000010.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
179.43.162.23	unknown	Panama		51852	PLI-ASCH	false

General Information

Joe Sandbox Version:	37.1.0 Beryl
Analysis ID:	877002
Start date and time:	2023-05-28 10:49:05 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 16s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	10
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
Sample file name:	09212399.exe
Detection:	MAL
Classification:	mal100.spyw.evad.winEXE@5/0@0/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 45.5% (good quality ratio 44%) • Quality average: 86.1% • Quality standard deviation: 23.7%

HCA Information:	Failed
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtQueryDirectoryFile 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

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):	7.379104304802616
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:	09212399.exe

File size:	503808
MD5:	57dd320eae0fadd155619407c8b5313c
SHA1:	fc2ce4b86d64025dbba19bb84e561a27fcb6ffb3
SHA256:	4a524e63c81e6cf9ab8a86f8de0973ea6a6d0973545867d34eba1b777e238628
SHA512:	23f1e1833a6a52d28cce3b07c726d568c2743b76593e46ba18cd97c7f3f29c262ea3624d7a3f0e745a6f776e0c21421e2a5a7541783fbcf1d31b359843436ddd
SSDEEP:	6144:e1z0CQa13pdiPumUtZVUqkj+VOVGakSEPhVHUk9ZuyxPwF7XgivTtiuy:eV0CQa131t1keBSEPHHUSu5tTtiuy
TLSH:	62B49E0392E53E54E9A68F769E1ED6E8760EF6708F193769311CBB1F08B0172D263B11
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....&...b...b...b...|.....|.....|...H...EX..k...b.....|...c...|...c...|...c...Richb.....PE..L.....pb.....

File Icon

Icon Hash:	454149454555691d

Static PE Info

General

Entrypoint:	0x404e59
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	NX_COMPAT, TERMINAL_SERVER_AWARE
Time Stamp:	0x6270CBC3 [Tue May 3 06:29:23 2022 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:	2d9ed3462f8a74bfd1231e2e9de56b43

Entrypoint Preview

Instruction
call 00007F2EE0CD8F13h
jmp 00007F2EE0CD45ADh
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
int3
mov ecx, dword ptr [esp+04h]
test ecx, 00000003h
je 00007F2EE0CD4756h
mov al, byte ptr [ecx]
add ecx, 01h
test al, al

Instruction
je 00007F2EE0CD4780h
test ecx, 00000003h
jne 00007F2EE0CD4721h
add eax, 00000000h
lea esp, dword ptr [esp+00000000h]
lea esp, dword ptr [esp+00000000h]
mov eax, dword ptr [ecx]
mov edx, 7EFEFEFFh
add edx, eax
xor eax, FFFFFFFFh
xor eax, edx
add ecx, 04h
test eax, 81010100h
je 00007F2EE0CD471Ah
mov eax, dword ptr [ecx-04h]
test al, al
je 00007F2EE0CD4764h
test ah, ah
je 00007F2EE0CD4756h
test eax, 00FF0000h
je 00007F2EE0CD4745h
test eax, FF000000h
je 00007F2EE0CD4734h
jmp 00007F2EE0CD46FFh
lea eax, dword ptr [ecx-01h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-02h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-03h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
lea eax, dword ptr [ecx-04h]
mov ecx, dword ptr [esp+04h]
sub eax, ecx
ret
mov edi, edi
push ebp
mov ebp, esp
sub esp, 20h
mov eax, dword ptr [ebp+08h]
push esi
push edi
push 00000008h
pop ecx
mov esi, 004012D8h
lea edi, dword ptr [ebp-20h]
rep movsd
mov dword ptr [ebp-08h], eax
mov eax, dword ptr [ebp+0Ch]
pop edi
mov dword ptr [ebp-04h], eax
pop esi

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	0x5c8b8	0x64	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x2a4000	0x19398	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x2be000	0xddc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x1220	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	0x3150	0x40	.text
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x1000	0x1d4	.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	0x5c37a	0x5c400	False	0.9075256182249323	data	7.890261806957562	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x5e000	0x245844	0x1e00	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rsrc	0x2a4000	0x19398	0x19400	False	0.37880956064356436	data	4.262404506795837	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x2be000	0x3540	0x3600	False	0.21788194444444445	data	2.444805500720407	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2a4730	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2a55d8	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2a5e80	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x2a8428	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2a94d0	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x2a9988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2aa830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2ab0d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x2ab640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x2adbe8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2aec90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		

Name	RVA	Size	Type	Language	Country
RT_ICON	0x2af618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x2afae8	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2b0990	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2b1238	0x6c8	Device independent bitmap graphic, 24 x 48 x 8, image size 0		
RT_ICON	0x2b1900	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x2b1e68	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x2b4410	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2b54b8	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_ICON	0x2b5988	0xea8	Device independent bitmap graphic, 48 x 96 x 8, image size 0		
RT_ICON	0x2b6830	0x8a8	Device independent bitmap graphic, 32 x 64 x 8, image size 0		
RT_ICON	0x2b70d8	0x568	Device independent bitmap graphic, 16 x 32 x 8, image size 0		
RT_ICON	0x2b7640	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 0		
RT_ICON	0x2b9be8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 0		
RT_ICON	0x2bac90	0x988	Device independent bitmap graphic, 24 x 48 x 32, image size 0		
RT_ICON	0x2bb618	0x468	Device independent bitmap graphic, 16 x 32 x 32, image size 0		
RT_STRING	0x2bbd20	0x664	data		
RT_STRING	0x2bc388	0x59e	data		
RT_STRING	0x2bc928	0x29a	data		
RT_STRING	0x2bcbc8	0x248	data		
RT_STRING	0x2bce10	0x582	data		
RT_GROUP_ICON	0x2bba80	0x68	data		
RT_GROUP_ICON	0x2a9938	0x4c	data		
RT_GROUP_ICON	0x2b5920	0x68	data		
RT_GROUP_ICON	0x2afa80	0x68	data		
RT_VERSION	0x2bbae8	0x238	data		

Imports

DLL	Import
KERNEL32.dll	GetModuleHandleW, IsBadReadPtr, GetConsoleAliasesLengthA, WaitForMultipleObjectsEx, GetPrivateProfileIntA, FreeConsole, GetVersionExW, WritePrivateProfileStructW, MulDiv, GetModuleFileNameW, CreateActCtxA, WritePrivateProfileStringW, ReplaceFileA, GetStringTypeExA, GetStdHandle, GetLogicalDriveStringsA, OpenMutexW, GetLastError, ReadConsoleOutputCharacterA, GetProcAddress, AttachConsole, SleepEx, VirtualAlloc, _hwrite, LoadLibraryA, InterlockedExchangeAdd, LocalAlloc, GetFileType, CreateFileMappingW, FindFirstVolumeMountPointW, GetNumberFormatW, CreateEventW, GetModuleFileNameA, lstrcmpiW, GetModuleHandleA, CreateMutexA, GetFileAttributesExW, GetConsoleCursorInfo, ScrollConsoleScreenBufferA, GetCurrentThreadId, FindAtomW, EnumResourceLanguagesW, DebugBreak, FindNextVolumeA, AddConsoleAliasW, CancelWaitableTimer, GetCommState, WaitForSingleObject, GetLongPathNameA, GetCommandLineA, GetStartupInfoA, RaiseException, RtlUnwind, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, HeapAlloc, HeapFree, WideCharToMultiByte, SetHandleCount, DeleteCriticalSection, EnterCriticalSection, LeaveCriticalSection, Sleep, ExitProcess, WriteFile, FreeEnvironmentStringsA, GetEnvironmentStrings, FreeEnvironmentStringsW, GetEnvironmentStringsW, TlsGetValue, TlsAlloc, TlsSetValue, TlsFree, InterlockedIncrement, SetLastError, InterlockedDecrement, HeapCreate, VirtualFree, QueryPerformanceCounter, GetTickCount, GetCurrentProcessId, GetSystemTimeAsFileTime, HeapReAlloc, SetFilePointer, GetConsoleCP, GetConsoleMode, GetCPInfo, GetACP, GetOEMCP, IsValidCodePage, InitializeCriticalSectionAndSpinCount, HeapSize, SetStdHandle, WriteConsoleA, GetConsoleOutputCP, WriteConsoleW, MultiByteToWideChar, LCMapStringA, LCMapStringW, GetStringTypeA, GetStringTypeW, GetLocaleInfoA, FlushFileBuffers, CreateFileA, CloseHandle
USER32.dll	CharLowerBuffA
GDI32.dll	GetCharWidthW, EnumFontsW, GetCharABCWidthsFloatW
ADVAPI32.dll	MapGenericMask

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:50:04.630919933 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.650755882 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.650926113 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.651165962 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.674498081 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.693221092 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.693255901 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.693388939 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.724514961 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.751171112 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.771742105 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.815829039 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.815866947 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.815884113 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.815896034 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.815908909 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.815922976 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.815941095 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.815958977 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.816119909 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.816183090 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.819185019 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.819215059 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.819232941 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.819246054 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.819405079 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.820241928 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.835942984 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.835977077 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.836178064 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.836520910 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.836540937 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.836616993 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.838181973 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.838207960 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.838315010 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.839436054 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.839459896 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.839526892 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.840878010 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.840904951 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.840981007 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.842473984 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.842500925 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.842591047 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.843739986 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.843764067 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.843849897 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.845112085 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.845136881 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.845201969 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.846401930 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.846425056 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.846472025 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.847753048 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.847779036 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.847822905 CEST	49699	8509	192.168.2.3	179.43.162.23

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 28, 2023 10:50:04.849085093 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.849116087 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.849148989 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.850456953 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.850481987 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.850521088 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.855834007 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.855906010 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.856055975 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.856076002 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.856158972 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.857459068 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.857484102 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.857537985 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.858748913 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.858772993 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.858870983 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.860100985 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.860122919 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.860203028 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.861520052 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.861543894 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.861619949 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.862901926 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.862926006 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.862996101 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.864188910 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.864213943 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.864324093 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.865366936 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.865391016 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.865478992 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.866457939 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.866480112 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.866554022 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.878592968 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.878631115 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.878655910 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.878675938 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.878695011 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.878695011 CEST	49699	8509	192.168.2.3	179.43.162.23
May 28, 2023 10:50:04.878714085 CEST	8509	49699	179.43.162.23	192.168.2.3
May 28, 2023 10:50:04.878734112 CEST	8509	49699	179.43.162.23	192.168.2.3

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 09212399.exe PID: **4968**, Parent PID: **3452**

General

Target ID:	0
Start time:	10:49:57
Start date:	28/05/2023
Path:	C:\Users\user\Desktop\09212399.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\09212399.exe
Imagebase:	0x400000
File size:	503808 bytes
MD5 hash:	57DD320EAE0FADD155619407C8B5313C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000003.364029125.0000000002632000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Smokeloader_3687686f, Description: unknown, Source: 00000000.00000002.381636049.00000000023D0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	low

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\SibCode	success or wait	1	27854A8	RegCreateKeyExW

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\SibCode	sn	dword	1685296200	success or wait	1	27854E7	RegSetValueExW

Analysis Process: certreq.exe PID: **7032**, Parent PID: **3452**

General

Target ID:	1
Start time:	10:50:01
Start date:	28/05/2023

Path:	C:\Windows\System32\certreq.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\certreq.exe
Imagebase:	0x7ff68c8c0000
File size:	517120 bytes
MD5 hash:	5A4F8BBCD943BC543B3F664C7DA83827
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\09212399.exe	success or wait	1	18822081B56	DeleteFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7064**, Parent PID: **7032**

General

Target ID:	2
Start time:	10:50:01
Start date:	28/05/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff745070000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: WerFault.exe PID: **3332**, Parent PID: **4968**

General

Target ID:	5
Start time:	10:50:08
Start date:	28/05/2023
Path:	C:\Windows\SysWOW64\WerFault.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\WerFault.exe -u -p 4968 -s 880
Imagebase:	0xef0000
File size:	434592 bytes
MD5 hash:	9E2B8ACAD48ECCA55C0230D63623661B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly