ID: 338144
Sample Name: 8QxrJSmRtc
Cookbook: default.jbs
Time: 17:59:11
Date: 11/01/2021
Version: 31.0.0 Red Diamond

Table of Contents

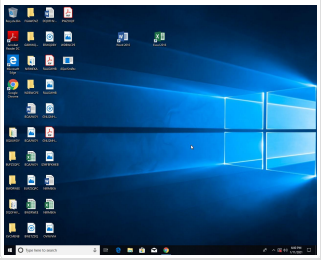
Analysis Report 8QxrJSmRtc

Overview

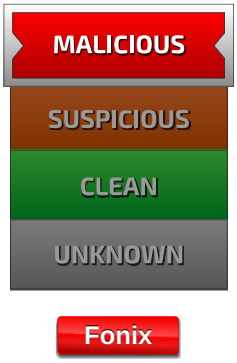
General Information

Sample Name:	8QxrJSmRtc (renamed file extension from none to exe)
Analysis ID:	338144
MD5:	6593b7ab157ac8..
SHA1:	c50e003f5c9ebee..
SHA256:	f8b132d8c750482.

Most interesting Screenshot:



Detection

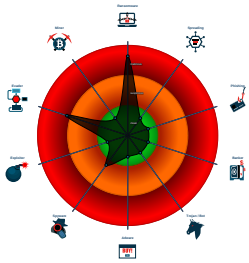


Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Multi AV Scanner detection for subm…
- Yara detected Fonix ransomware
- Yara detected Ransomware_Generic
- Deletes shadow drive data (may be …
- May drop file containing decryption i…
- Tries to detect sandboxes and other…
- Contains functionality to check if a d…
- Contains functionality to check if a d…
- Contains functionality to query locale…
- Detected potential crypto function
- Extensive use of GetProcAddress (o…

Classification



Startup

- **System is w10x64**
- 8QxrJSmRtc.exe (PID: 6768 cmdline: 'C:\Users\user\Desktop\8QxrJSmRtc.exe' MD5: 6593B7AB157AC82967AF0E92EFA96134)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
8QxrJSmRtc.exe	JoeSecurity_Ransomware_Generic	Yara detected Ransomware_Generic	Joe Security	
8QxrJSmRtc.exe	JoeSecurity_Fonix	Yara detected Fonix ransomware	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000000.646603344.000000000147D000.00000002.00020000.sdmp	JoeSecurity_Ransomware_Generic	Yara detected Ransomware_Generic	Joe Security	
00000000.00000000.646603344.000000000147D000.00000002.00020000.sdmp	JoeSecurity_Fonix	Yara detected Fonix ransomware	Joe Security	
00000000.00000002.657343156.000000000147D000.00000002.00020000.sdmp	JoeSecurity_Ransomware_Generic	Yara detected Ransomware_Generic	Joe Security	
00000000.00000002.657343156.000000000147D000.00000002.00020000.sdmp	JoeSecurity_Fonix	Yara detected Fonix ransomware	Joe Security	
Process Memory Space: 8QxrJSmRtc.exe PID: 6768	JoeSecurity_Ransomware_Generic	Yara detected Ransomware_Generic	Joe Security	

Click to see the 1 entries

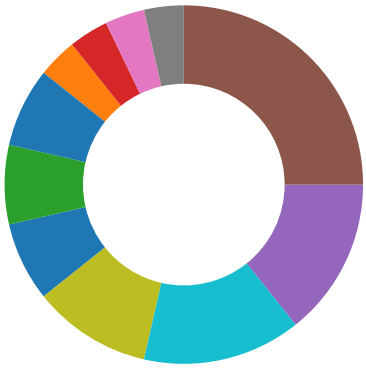
Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.8QxrJSmRtc.exe.13b0000.0.unpack	JoeSecurity_Ransomware_Generic	Yara detected Ransomware_Generic	Joe Security	
0.2.8QxrJSmRtc.exe.13b0000.0.unpack	JoeSecurity_Fonix	Yara detected Fonix ransomware	Joe Security	
0.0.8QxrJSmRtc.exe.13b0000.0.unpack	JoeSecurity_Ransomware_Generic	Yara detected Ransomware_Generic	Joe Security	
0.0.8QxrJSmRtc.exe.13b0000.0.unpack	JoeSecurity_Fonix	Yara detected Fonix ransomware	Joe Security	

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Cryptography
- Compliance
- Networking
- Spam, unwanted Advertisements and Ransom Demands
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Spam, unwanted Advertisements and Ransom Demands:

Yara detected Fonix ransomware

Yara detected Ransomware_Generic

Deletes shadow drive data (may be related to ransomware)

May drop file containing decryption instructions (likely related to ransomware)

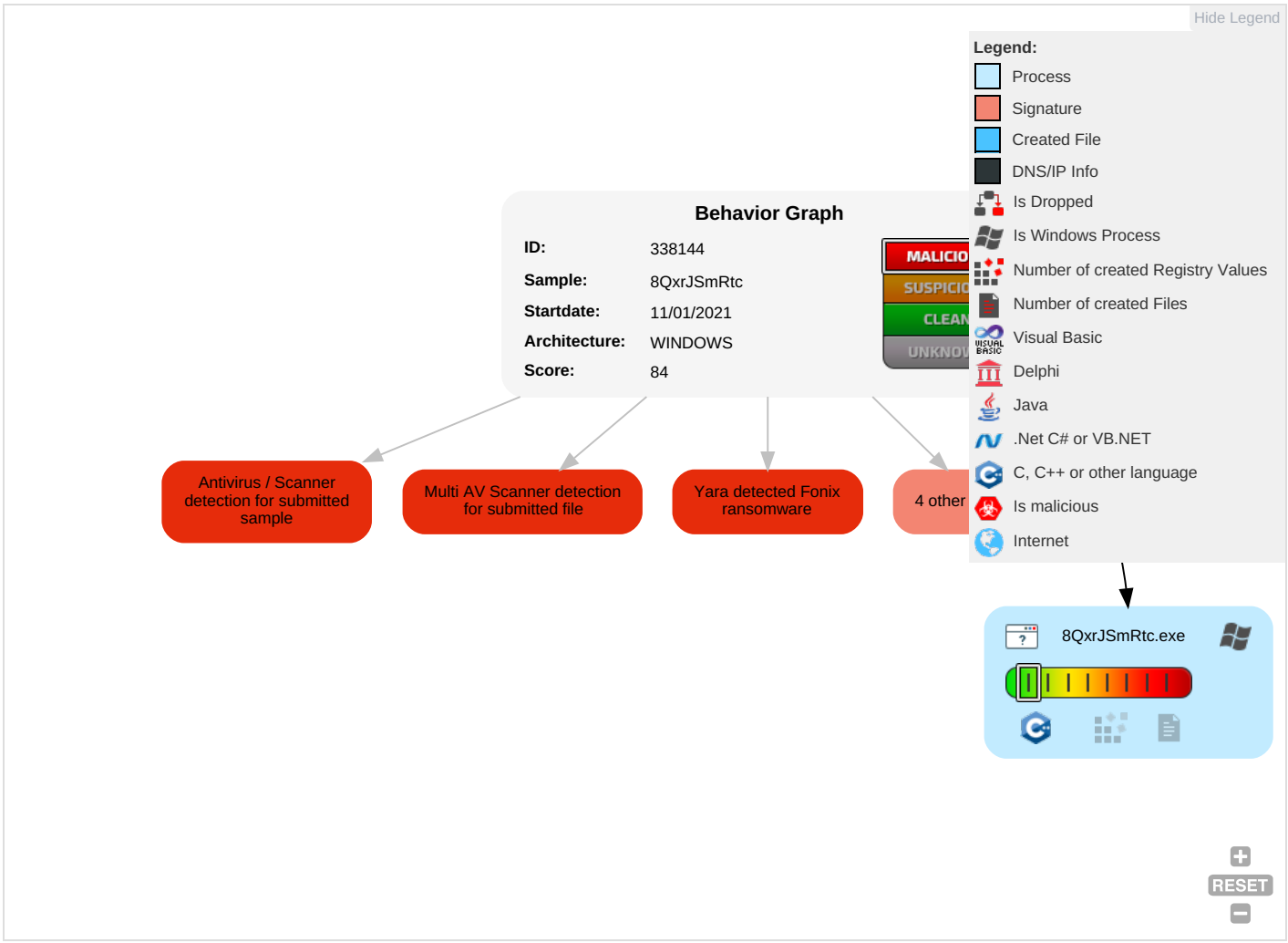
Malware Analysis System Evasion:

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

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
Valid Accounts	Windows Management Instrumentation	Application Shimming 1	Application Shimming 1	File Deletion 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	Security Software Discovery 1 2 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	System Information Discovery 1 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups

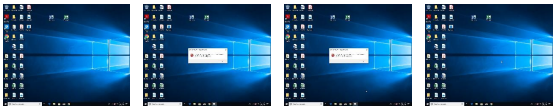
Behavior Graph



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
8QxrJSmRtc.exe	41%	Virustotal		Browse
8QxrJSmRtc.exe	59%	ReversingLabs	Win64.Ransomware.Fonix	
8QxrJSmRtc.exe	100%	Avira	HEUR/AGEN.1138883	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.8QxrJSmRtc.exe.13b0000.0.unpack	100%	Avira	HEUR/AGEN.1138883		Download File
0.2.8QxrJSmRtc.exe.13b0000.0.unpack	100%	Avira	HEUR/AGEN.1138883		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://uupload.ir/files/g510_windows_10.gif	8QxrJSmRtc.exe	false		high
http://https://www.who.int	8QxrJSmRtc.exe	false		high
http://https://code.jquery.com/jquery-latest.js	8QxrJSmRtc.exe	false		high

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	338144
Start date:	11.01.2021
Start time:	17:59:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	8QxrJSmRtc (renamed file extension from none 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:	1
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:	mal84.rans.evad.winEXE@1/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32+ executable (console) x86-64, for MS Windows
Entropy (8bit):	6.349484774601221
TrID:	• Win64 Executable Console (202006/5) 92.65% • Win64 Executable (generic) (12005/4) 5.51% • Generic Win/DOS Executable (2004/3) 0.92% • DOS Executable Generic (2002/1) 0.92% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	8QxrJSmRtc.exe
File size:	1266176
MD5:	6593b7ab157ac82967af0e92efa96134
SHA1:	c50e003f5c9ebeebc798b6f00b09aae05518d6cf
SHA256:	f8b132d8c750482bd5b6f03bae58f6805fb3480ef0904a21f0111ede5a1ebb1b
SHA512:	2028cbd94372a900ada0a5daeb68a7608e2013adcac4750c36979d137e4c29b3c5a3e524b42e6b4563ad6d27b5990881f2fdab3ede5b1296ec4c4fb96cc0bbc6
SSDEEP:	24576:z9C4QYc8ntZP2sQQ0GqrCPQX8BYOzhjZAJZ1o:z9C4PnnP5QQ0xrj8Cshir
File Content Preview:	MZ.....@.....(.....!..L.!This program cannot be run in DOS mode....$.....}P^...^.....^.....J.....S.....;._.....O.....T.....Q...^.....r.....\....._.....^..._..

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4729a4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows cui
Image File Characteristics:	EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x5FF0BEEA [Sat Jan 2 18:43:54 2021 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:	0c0d7ab54c9443fe1117b1f5373e7fb1

Entrypoint Preview

Instruction
dec eax
sub esp, 28h
call 00007F2978719178h
dec eax
add esp, 28h
jmp 00007F2978718797h
int3
int3
dec eax
sub esp, 28h
dec ebp
mov eax, dword ptr [ecx+38h]
dec eax
mov ecx, edx
dec ecx
mov edx, ecx
call 00007F2978718932h
mov eax, 00000001h
dec eax
add esp, 28h
ret
int3
int3
int3
inc eax
push ebx
inc ebp
mov ebx, dword ptr [eax]
dec eax
mov ebx, edx
inc ecx
and ebx, FFFFFFF8h
dec esp
mov ecx, ecx
inc ecx
test byte ptr [eax], 00000004h
dec esp

Instruction
mov edx, ecx
je 00007F2978718935h
inc ecx
mov eax, dword ptr [eax+08h]
dec ebp
arpl word ptr [eax+04h], dx
neg eax
dec esp
add edx, ecx
dec eax
arpl ax, cx
dec esp
and edx, ecx
dec ecx
arpl bx, ax
dec edx
mov edx, dword ptr [eax+edx]
dec eax
mov eax, dword ptr [ebx+10h]
mov ecx, dword ptr [eax+08h]
dec eax
mov eax, dword ptr [ebx+08h]
test byte ptr [ecx+eax+03h], 0000000Fh
je 00007F297871892Dh
movzx eax, byte ptr [ecx+eax+03h]
and eax, FFFFFFF0h
dec esp
add ecx, eax
dec esp
xor ecx, edx
dec ecx
mov ecx, ecx
pop ebx
jmp 00007F2978717FD2h
int3
dec eax
mov eax, esp
dec eax
mov dword ptr [eax+08h], ebx
dec eax
mov dword ptr [eax+10h], ebp
dec eax
mov dword ptr [eax+18h], esi
dec eax
mov dword ptr [eax+20h], edi
inc ecx
push esi
dec eax
sub esp, 20h
dec ecx
mov ebx, dword ptr [ecx+38h]
dec eax
mov esi, edx
dec ebp
mov esi, eax
dec eax
mov ebp, ecx
dec ecx
mov edx, ecx
dec eax
mov ecx, esi
dec ecx
mov edi, ecx
dec esp

Instruction
lea eax, dword ptr [ebx+04h]
call 00007F2978718891h

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x11f698	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x138000	0x1e0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x12d000	0x9de0	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0xffc60	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0xffb30	0x130	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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	0xcba04	0xcbc00	False	0.472408215107	data	6.42014647338	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xcd000	0x53938	0x53a00	False	0.40311448991	data	5.43180771387	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x121000	0xbd4c	0x8a00	False	0.188688858696	data	4.87188898109	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.pdata	0x12d000	0x9de0	0x9e00	False	0.485289754747	data	5.98253637707	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
_RDATA	0x137000	0x94	0x200	False	0.20703125	data	1.38531860657	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x138000	0x1e0	0x200	False	0.529296875	data	4.71229819329	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x139000	0x2ba0	0x2c00	False	0.00301846590909	data	0.0	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x138060	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import

DLL	Import
KERNEL32.DLL	SetThreadPriority, CreateMutexW, InitializeCriticalSectionEx, FindClose, LocalAlloc, ReleaseMutex, GetLocaleInfoA, OpenProcess, SetFileAttributesW, CreateToolhelp32Snapshot, Sleep, FormatMessageW, CopyFileA, GetLastError, Process32NextW, DeleteFileA, Process32FirstW, CloseHandle, RaiseException, DecodePointer, GetDriveTypeA, LocalFree, DeleteCriticalSection, CopyFileW, WideCharToMultiByte, GetConsoleWindow, GetDiskFreeSpaceExA, OpenMutexW, GetDriveTypeW, SetLastError, QueryPerformanceCounter, QueryPerformanceFrequency, GetCurrentThread, GetThreadTimes, SetEndOfFile, WriteConsoleW, CreateFileW, SetStdHandle, GetProcessHeap, SetEnvironmentVariableW, TerminateProcess, GetCurrentProcess, FindNextFileW, SetPriorityClass, FindFirstFileW, SetThreadPriorityBoost, SetProcessPriorityBoost, FreeEnvironmentStringsW, GetEnvironmentStringsW, GetOEMCP, GetACP, IsValidCodePage, FindFirstFileExW, HeapSize, HeapReAlloc, ReadConsoleW, ReadFile, GetFileAttributesExW, CreateProcessW, GetExitCodeProcess, GetConsoleMode, GetConsoleCP, MultiByteToWideChar, GetStringTypeW, EnterCriticalSection, LeaveCriticalSection, TryEnterCriticalSection, GetCurrentThreadId, WaitForSingleObjectEx, SwitchToThread, EncodePointer, InitializeCriticalSectionAndSpinCount, CreateEventW, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, GetSystemTimeAsFileTime, GetTickCount, GetModuleHandleW, GetProcAddress, CompareStringW, LCMapStringW, GetLocaleInfoW, GetCPInfo, IsDebuggerPresent, OutputDebugStringW, SetEvent, ResetEvent, InitializeSListHead, RtlCaptureContext, RtlLookupFunctionEntry, RtlVirtualUnwind, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsProcessorFeaturePresent, GetStartupInfoW, GetCurrentProcessId, CreateTimerQueue, SignalObjectAndWait, CreateThread, GetThreadPriority, GetLogicalProcessorInformation, CreateTimerQueueTimer, ChangeTimerQueueTimer, DeleteTimerQueueTimer, GetNumaHighestNodeNumber, GetProcessAffinityMask, SetThreadAffinityMask, RegisterWaitForSingleObject, UnregisterWait, FreeLibrary, FreeLibraryAndExitThread, GetModuleFileNameW, GetModuleHandleA, LoadLibraryExW, GetVersionExW, VirtualAlloc, VirtualProtect, VirtualFree, DuplicateHandle, ReleaseSemaphore, InterlockedPopEntrySList, InterlockedPushEntrySList, InterlockedFlushSList, QueryDepthSList, UnregisterWaitEx, LoadLibraryW, WaitForSingleObject, RtlUnwindEx, RtlPcToFileHeader, ExitProcess, GetModuleHandleExW, ExitThread, MoveFileExW, GetStdHandle, WriteFile, GetCommandLineA, GetCommandLineW, GetFileSizeEx, SetFilePointerEx, GetFileType, HeapAlloc, HeapFree, IsValidLocale, GetUserDefaultLCID, EnumSystemLocalesW, FlushFileBuffers, RtlUnwind
ADVAPI32.dll	CryptAcquireContextA, CryptGenRandom, CryptReleaseContext, GetUserNameA
IPHLPAPI.DLL	GetIpNetTable
NETAPI32.dll	NetShareEnum, NetApiBufferFree
USER32.dll	GetKeyboardLayoutList, ShowWindow, MessageBoxW, SystemParametersInfoW
WININET.dll	InternetCheckConnectionA
WS2_32.dll	inet_ntoa, socket, connect, WSAGetLastError, send, WSAStartup, gethostbyname, closesocket, WSACleanup, recv, htons

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

System Behavior

Analysis Process: 8QxrJSmRtc.exe PID: 6768 Parent PID: 6076

General

Start time:	17:59:58

Start date:	11/01/2021
Path:	C:\Users\user\Desktop\8QxrJSmRtc.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\8QxrJSmRtc.exe'
Imagebase:	0x13b0000
File size:	1266176 bytes
MD5 hash:	6593B7AB157AC82967AF0E92EFA96134
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Ransomware_Generic, Description: Yara detected Ransomware_Generic, Source: 00000000.00000000.646603344.000000000147D000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Fonix, Description: Yara detected Fonix ransomware, Source: 00000000.00000000.646603344.000000000147D000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Ransomware_Generic, Description: Yara detected Ransomware_Generic, Source: 00000000.00000002.657343156.000000000147D000.00000002.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Fonix, Description: Yara detected Fonix ransomware, Source: 00000000.00000002.657343156.000000000147D000.00000002.00020000.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis