Summary

File Name: java.exe

File Type: PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows

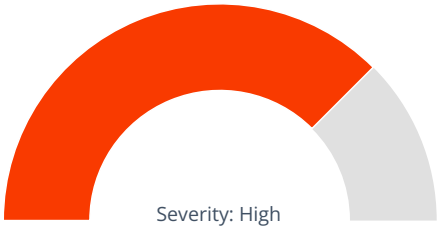
SHA1: 54bcf774774d5a64bb0f7641325f381443a5dfca

MD5: c7ace8d52dbc590cb25b467528eb72b7

MALWARE

Xcitium Verdict Cloud Final Verdict

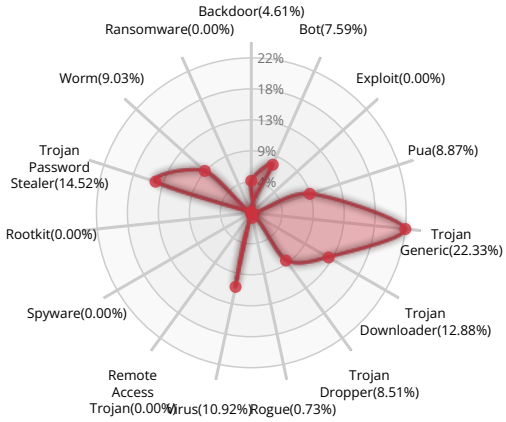
DETECTION SECTION



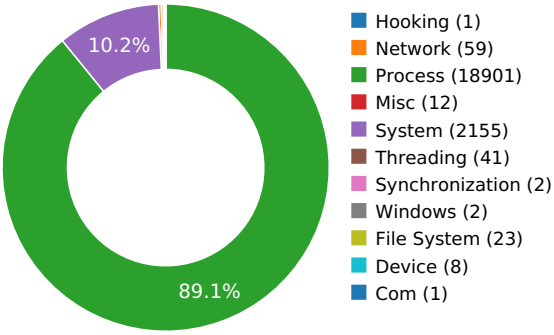
Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

The executable is compressed using UPX Show sources

INFORMATION DISCOVERY

Expresses interest in specific running processes Show sources

Repeatedly searches for a not-found process, may want to run with startbrowser=1 option

NETWORKING

Attempts to connect to a dead IP:Port (2 unique times) Show sources

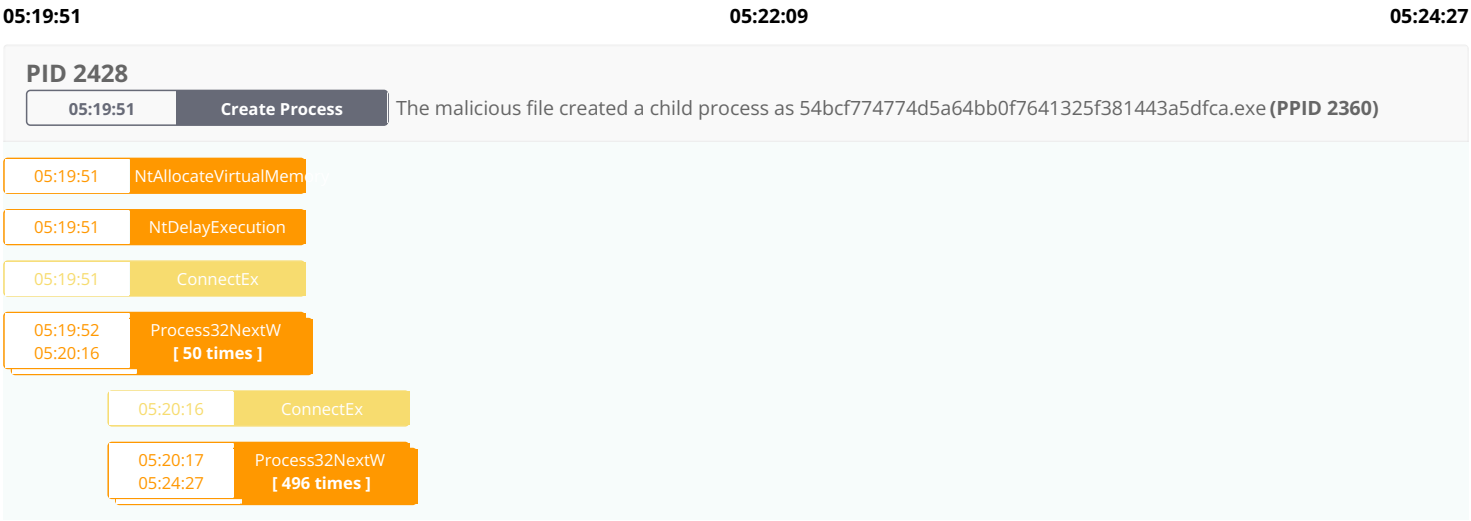
MALWARE ANALYSIS SYSTEM EVASION

A process attempted to delay the analysis task. Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Behavior Graph



Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Windows\sysnative\WSHTCPIP.DLL
C:\Windows\sysnative\wship6.dll
C:\Windows\sysnative\wshqos.dll
C:\Program Files\Common Files\SSL\openssl.cnf

RESOLVED APIS

kernel32.dll.QueryPerformanceFrequency
kernel32.dll.QueryPerformanceCounter
kernel32.dll.SizeofResource
kernel32.dll.LockResource
kernel32.dll.LoadResource
kernel32.dll.FindResourceW
kernel32.dll.GetConsoleWindow
kernel32.dll.CreateMutexW
kernel32.dll.GetLastError
kernel32.dll.GetSystemFirmwareTable
kernel32.dll.HeapFree
kernel32.dll.HeapAlloc
kernel32.dll.GetProcessHeap
kernel32.dll.MultiByteToWideChar
kernel32.dll.SetPriorityClass
kernel32.dll.GetCurrentProcess
kernel32.dll.SetThreadPriority
kernel32.dll.GetSystemPowerStatus
kernel32.dll.GetCurrentThread
kernel32.dll.GetProcAddress
kernel32.dll.GetModuleHandleW
kernel32.dll.GetThreadTimes
kernel32.dll.GetTickCount
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.Sleep
kernel32.dll.Process32NextW

kernel32.dll.Process32FirstW
kernel32.dll.CloseHandle
kernel32.dll.FreeConsole
kernel32.dll.VirtualProtect
kernel32.dll.VirtualFree
kernel32.dll.VirtualAlloc
kernel32.dll.GetLargePageMinimum
kernel32.dll.LocalAlloc
kernel32.dll.LocalFree
kernel32.dll.FlushInstructionCache
kernel32.dll.WaitForSingleObject
kernel32.dll.CreateEventW
kernel32.dll.SetEvent
kernel32.dll.GetCurrentThreadId
kernel32.dll.AddVectoredExceptionHandler
kernel32.dll.DeviceIoControl
kernel32.dll.CreateFileW
kernel32.dll.SetLastError
kernel32.dll.GetSystemTime
kernel32.dll.SystemTimeToFileTime
kernel32.dll.GetModuleHandleExW
kernel32.dll.EnterCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.InitializeCriticalSectionAndSpinCount
kernel32.dll.DeleteCriticalSection
kernel32.dll.TlsAlloc
kernel32.dll.TlsGetValue
kernel32.dll.TlsSetValue
kernel32.dll.TlsFree
kernel32.dll.SwitchToFiber
kernel32.dll.DeleteFiber
kernel32.dll.CreateFiber
kernel32.dll.FindClose
kernel32.dll.FindFirstFileW
kernel32.dll.FindNextFileW

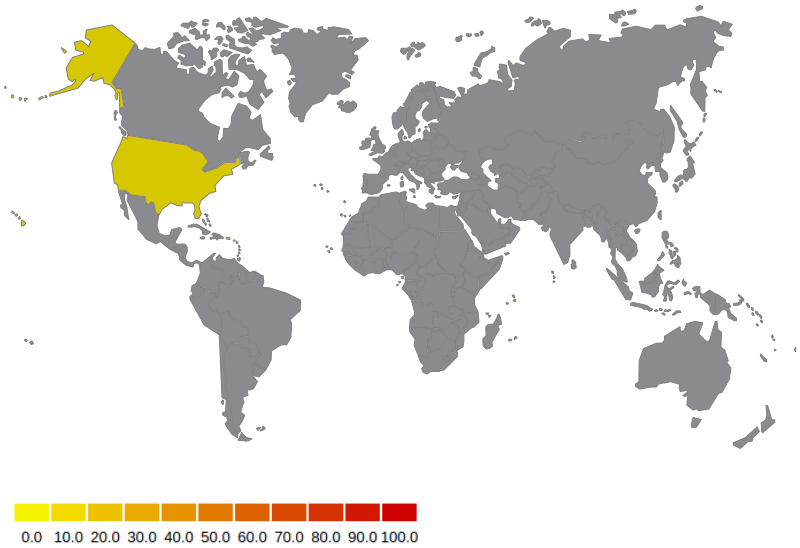
kernel32.dll.WideCharToMultiByte
kernel32.dll.GetFileType
kernel32.dll.WriteFile
kernel32.dll.ConvertFiberToThread
kernel32.dll.ConvertThreadToFiber
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.FreeLibrary
kernel32.dll.LoadLibraryA
kernel32.dll.LoadLibraryW
kernel32.dll.GetEnvironmentVariableW
kernel32.dll.ReadConsoleA
kernel32.dll.ReadConsoleW
kernel32.dll.PostQueuedCompletionStatus
kernel32.dll.CreateFileA

READ FILES

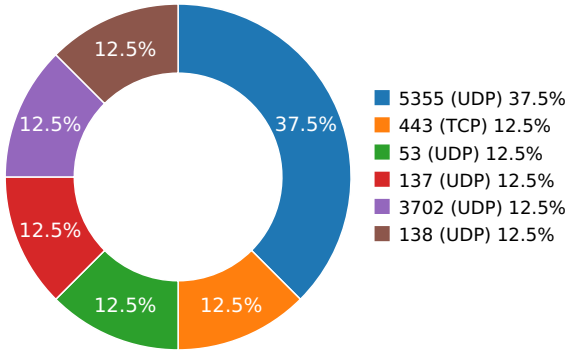
\Device\KsecDD
C:\Windows\sysnative\wship6.dll
C:\Windows\sysnative\wshqos.dll
C:\Program Files\Common Files\SSL\openssl.cnf

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	185.10.68.220	Seychelles	200651	Not known	Malware Process
	109.71.252.45		213250	Not known	Malware Process
eu.minerpool.pw	107.182.129.82	United States	211252	Serverion LLC	Malware Process

DNS QUERIES

Request	Type
eu.minerpool.pw	A

Answers
- 185.10.68.123 (A)
- 109.71.252.45 (A)
- 107.182.129.82 (A)
- 185.10.68.220 (A)

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
34.7660219669	Sandbox	185.10.68.220	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.77580499649	Sandbox	224.0.0.252	5355
6.77638292313	Sandbox	224.0.0.252	5355
6.78634691238	Sandbox	239.255.255.250	3702
6.80484890938	Sandbox	192.168.56.255	137
9.35859489441	Sandbox	224.0.0.252	5355
9.5472509861	Sandbox	8.8.4.4	53
12.803716898	Sandbox	192.168.56.255	138

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	java.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
SHA1:	54bcf774774d5a64bb0f7641325f381443a5dfca
MD5:	c7ace8d52dbc590cb25b467528eb72b7
First Seen Date:	2023-07-02 09:05:08.654716 (3 days ago)
Number Of Clients Seen:	3
Last Analysis Date:	2023-07-02 21:28:55.939511 (3 days ago)
Human Expert Analysis Date:	2023-07-03 10:20:41.088566 (2 days ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	4
File Type Enum	7
Debug Artifacts	[]
Number Of Sections	3
Trid	[[87.1, u'UPX compressed Win32 Executable'], [6.4, u'Generic Win/DOS Executable'], [6.4, u'DOS Executable Generic']]
Compilation Time Stamp	0x64A144E9 [Sun Jul 2 09:35:37 2023 UTC]
LegalCopyright	Copyright \xc2\xa9 2018
FileVersion	1.8.0_171-b11
CompanyName	
ProductName	Java(TM) Platform SE 8
ProductVersion	1.8.0_171-b11
FileDescription	Java(TM) Platform SE binary
OriginalFilename	java.exe
Translation	0x0000 0x04b0
Entry Point	0x140740ea0 (UPX1)
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
File Size	1638400
Ssdeep	49152:GXt17+Rfj3ppdpZjoNcUT93rADmMvRkvuYZ7D6:GaVjDhUNc299CuD6
Sha256	8af4b8a734f28ee133c6a388bc8737b414532a8294d5a6f095cd8f0fe0a113ef
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/5/4/b/c/54bcf774774d5a64bb0f7641325f381443a5dfca', u'EXE:OriginalFileName': u'java.exe', u'EXE:ProductName': u'Java(TM) Platform SE 8', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:07:02 09:04:26+00:00', u'EXE:InitializedDataSize': 12288, u'File:FileModifyDate': u'2023:07:02 09:04:26+00:00', u'EXE:FileVersionNumber': u'3.3.1.0', u'EXE:FileVersion': u'1.8.0_171-b11', u'File:FileSize': u'1600 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'AMD AMD64', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1.8.0_171-b11', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win64 EXE', u'EXE:CompanyName': u'', u'File:FileName': u'54bcf774774d5a64bb0f7641325f381443a5dfca', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 6.0, u'EXE:PEType': u'PE32+', u'EXE:TimeStamp': u'2023:07:02 09:35:37+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xc2\xa9 2018', u'EXE:LinkerVersion': 14.29, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/5/4/b/c', u'EXE:FileDescription': u'Java(TM) Platform SE binary', u'EXE:EntryPoint': u'0x740ea0', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 1626112, u'File:FileInodeChangeDate': u'2023:07:02 09:04:26+00:00', u'EXE:UninitializedDataSize': 5980160, u'EXE:LanguageCode': u'Neutral', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'3.3.1.0'}]
Mime Type	application/x-dosexec
Imphash	bb388b5fb16beacfa2a7403d25eaa8c4

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x5b4000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0x5b5000	0x18d000	0x18ce00	7.99978751176	3e8cdb9544e42c7fa85a73c2acec4e45
.rsrc	0x742000	0x3000	0x2e00	5.67580083649	a5e68c44143c4320ccf9f337f19dddee

PE Imports

- ADVAPI32.dll
  - LsaClose
- bcrypt.dll
  - BCryptGenRandom
- CRYPT32.dll
  - CertOpenStore
- IPHLPAPI.DLL
  - GetAdaptersAddresses
- KERNEL32.DLL
  - LoadLibraryA
  - ExitProcess
  - GetProcAddress
  - VirtualProtect
- ole32.dll
  - CoInitializeEx
- PSAPI.DLL
  - GetProcessMemoryInfo
- USER32.dll
  - ShowWindow
- USERENV.dll
  - GetUserProfileDirectoryW
- WS2_32.dll
  - ioctlsocket

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 7610676, u'sha256': u'752046db2d5ba9b48214cfdc907886277a63ca3638eb1d38a00f207878da0a7d', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 7620320, u'sha256': u'6eb54801f91b6d8effccbfaefe6b2d7705a274a75940e6226e24e0d4ec58c396', u'type': u'MS Windows icon resource - 1 icon, 48x48', u'size': 20}

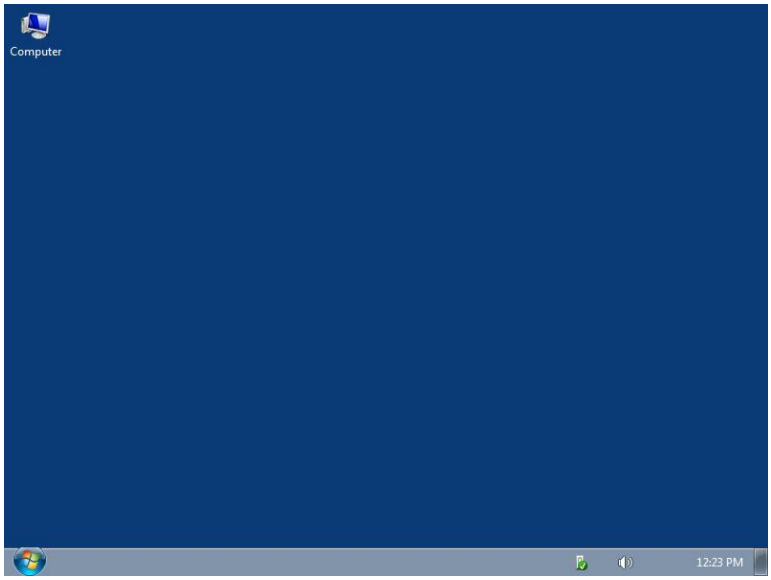
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 7620344, u'sha256': u'337dcde727e6203f36765a9d8cce1e0f3dab983cd4921bb10481dd49e476b009', u'type': u'data', u'size': 684}

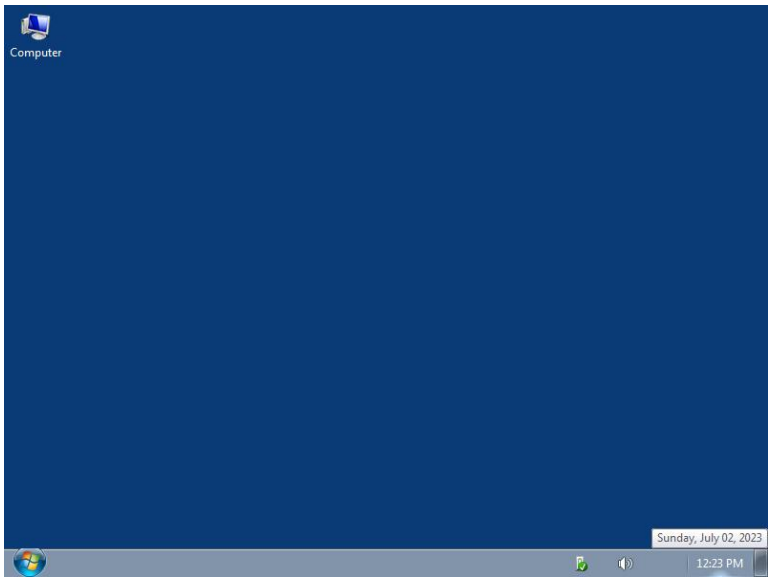
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 7621032, u'sha256': u'49a60be4b95b6d30da355a0c124af82b35000bce8f24f957d1c09ead47544a1e', u'type': u'ASCII text, with CRLF line terminators', u'size': 346}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS


Computer
12:23 PM


Computer
Sunday, July 02, 2023
12:23 PM


Computer
12:19 PM