VALKYRIE COMODO

Summary

File Name: services.exe

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

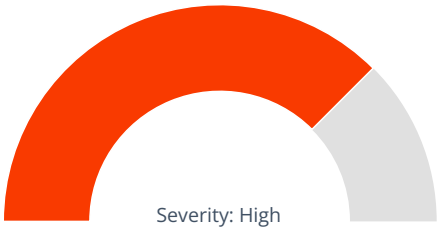
SHA1: 44a3eaf1e91ac124b950dceaf870c5cb574403c0

MD5: 059bff8c2b8b17074a8244b83a0e5064

MALWARE

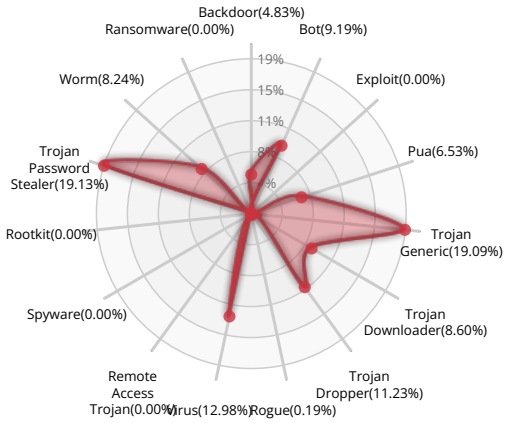
Valkyrie Final Verdict

DETECTION SECTION

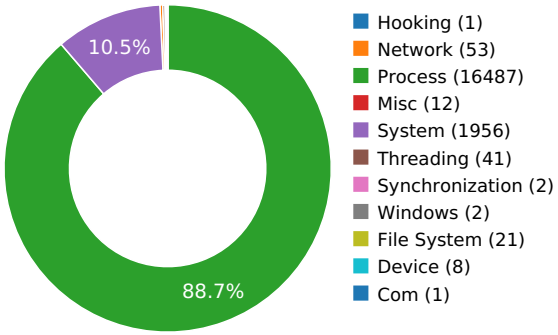


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

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

STATIC ANOMALY

Unusual version info supplied for binary Show sources

NETWORKING

Attempts to connect to a dead IP:Port (1 unique times) Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Behavior Graph

VALKYRIE COMODO

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

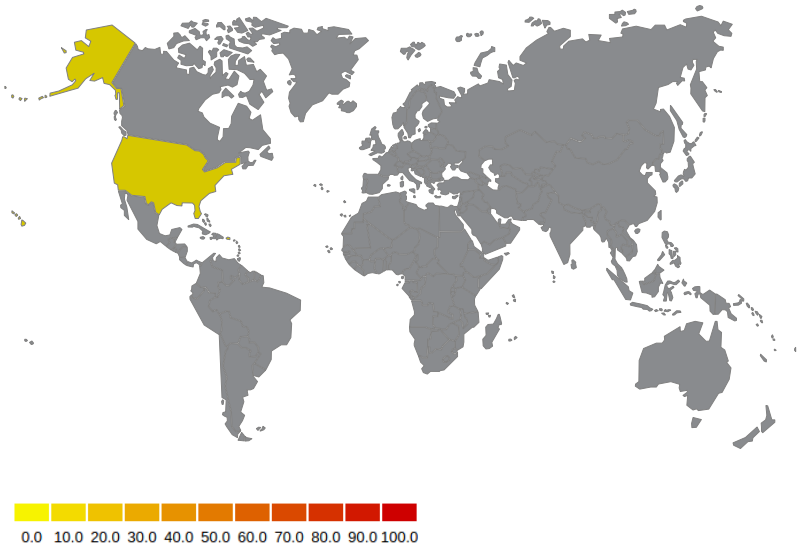
kernel32.dll.WideCharToMultiByte
kernel32.dll.GetFileType
kernel32.dll.WriteFile
kernel32.dll.ConvertFiberToThread
kernel32.dll.ConvertThreadToFiber
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetSystemTimeAsFileTime
kernel32.dll.FreeLibrary
kernel32.dll.LoadLibraryA
kernel32.dll.LoadLibraryW
kernel32.dll.GetEnvironmentVariableW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

READ FILES

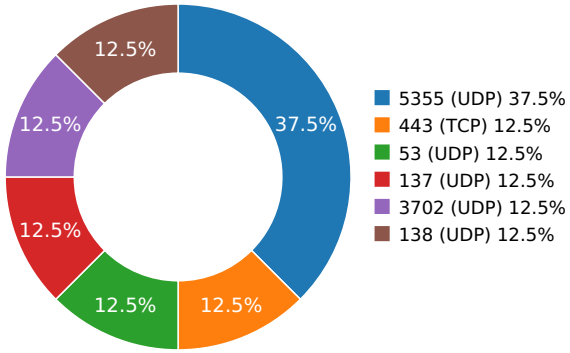
\Device\KsecDD
C:\Windows\sysnative\wship6.dll
C:\Windows\sysnative\wshqos.dll
C:\Program Files\Common Files\SSL\openssl.cnf

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
eu.minerpool.pw	185.10.68.220	Seychelles	200651	Not known	Malware Process

DNS QUERIES

Request	Type
eu.minerpool.pw	A
Answers - 185.10.68.123 (A) - 107.182.129.82 (A) - 109.71.252.45 (A) - 185.10.68.220 (A)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
9.80543398857	Sandbox	185.10.68.220	443

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.82141089439	Sandbox	224.0.0.252	5355
6.82195496559	Sandbox	224.0.0.252	5355
6.83688402176	Sandbox	239.255.255.250	3702
6.87338805199	Sandbox	192.168.56.255	137
9.3892159462	Sandbox	224.0.0.252	5355
9.54917407036	Sandbox	8.8.4.4	53
12.8729128838	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	services.exe
File Type:	PE32+ executable (GUI) x86-64 (stripped to external PDB), for MS Windows
SHA1:	44a3eaf1e91ac124b950dceaf870c5cb574403c0
MD5:	059bff8c2b8b17074a8244b83a0e5064
First Seen Date:	2023-07-01 10:57:31.076012 (2 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2023-07-02 20:15:34.188225 (2 years ago)
Human Expert Analysis Date:	2023-07-02 11:50:13.805692 (2 years ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

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	0x64A008FD [Sat Jul 1 11:07:41 2023 UTC]
LegalCopyright	\xa9 Microsoft Corporation. All rights reserved.
FileVersion	10.0.17134.1 (WinBuild.160101.0800)
CompanyName	
ProductName	Services and Controller app
ProductVersion	10.0.17134.1 (WinBuild.160101.0800)
FileDescription	Services and Controller app
OriginalFilename	service.exe
Translation	0x0000 0x04b0
Entry Point	0x14073eb20 (UPX1)
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
File Size	1631744
Ssdeep	49152:QE7xMPyJsGj8senhOMC8zVve9uuu7vNZO:tM6fMOMguF7vNZ
Sha256	0ef6fb2827f5a470de72dd1355a8aa51e12c073386b4a1a8d4fc064ec7dd74fe
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/4/4/a/3/44a3eaf1e91ac124b950dceaf870c5cb574403c0', u'EXE:OriginalFileName': u'service.exe', u'EXE:ProductName': u'Services and Controller app', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:07:02 20:15:21+00:00', u'EXE:InitializedDataSize': 4096, u'File:FileModifyDate': u'2023:07:01 10:56:58+00:00', u'EXE:FileVersionNumber': u'3.3.1.0', u'EXE:FileVersion': u'10.0.17134.1 (WinBuild.160101.0800)', u'File:FileSize': u'1594 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'AMD AMD64', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'10.0.17134.1 (WinBuild.160101.0800)', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win64 EXE', u'EXE:CompanyName': u'', u'File:FileName': u'44a3eaf1e91ac124b950dceaf870c5cb574403c0', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 6.0, u'EXE:PEType': u'PE32+', u'EXE:TimeStamp': u'2023:07:01 11:07:41+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'\xa9 Microsoft Corporation. All rights reserved.', 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/4/4/a/3', u'EXE:FileDescription': u'Services and Controller app', u'EXE:EntryPoint': u'0x73eb20', u'EXE:SubsystemVersion': 6.0, u'EXE:CodeSize': 1630208, u'File:FileInodeChangeDate': u'2023:07:01 10:56:58+00:00', u'EXE:UninitializedDataSize': 5967872, 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	0x5b1000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0x5b2000	0x18e000	0x18da00	7.99979080901	8a647a8dfb6398d23aa5341fd5984762
.rsrc	0x740000	0x1000	0xa00	3.77523195089	181caf0ce0581d47728db936a5e87372

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_VERSION', u'offset': 7602340, u'sha256': u'f6e26c5118f64b8c8d3eb6c35430f2ca09e67cc58fa3068ae3d33a5b1cd23066', u'type': u'data', u'size': 840}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 7603184, u'sha256': u'49a60be4b95b6d30da355a0c124af82b35000bce8f24f957d1c09ead47544a1e', u'type': u'ASCII text, with CRLF line terminators', u'size': 346}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS