VALKYRIE COMODO

Summary

File Name: readme.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

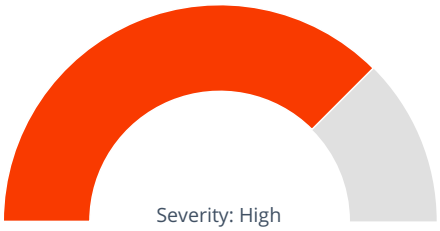
SHA1: faf73abf89f0df908254e72c3fb02eaf0a8f5ddc

MD5: 4cbf5af84e0424aeb79910b840d893b1

MALWARE

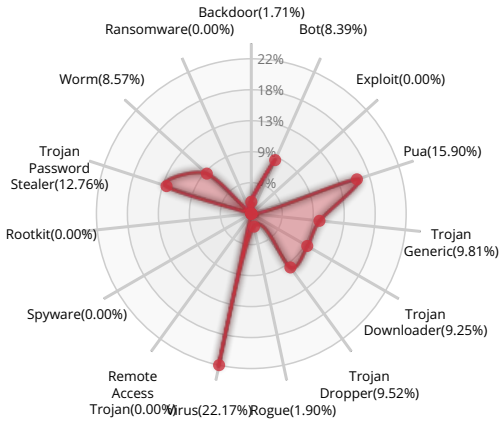
Valkyrie Final Verdict

DETECTION SECTION

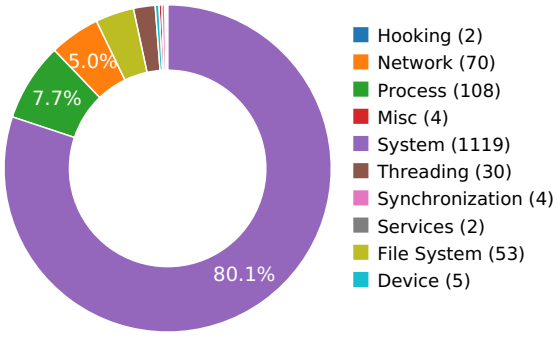


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

INFORMATION DISCOVERY

Attempts to remove evidence of file being downloaded from the Internet Show sources

NETWORKING

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

HTTP traffic contains suspicious features which may be indicative of malware related traffic Show sources

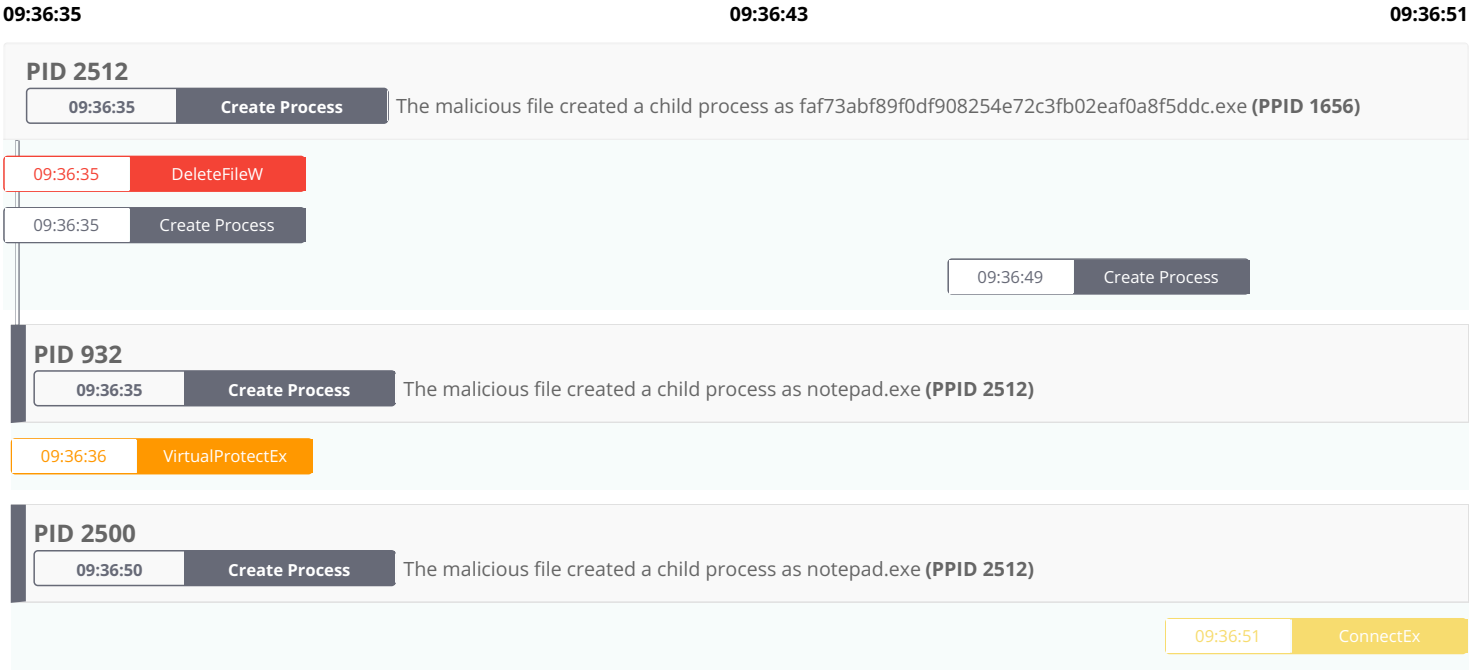
Performs some HTTP requests Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

VALKYRIE COMODO

Behavior Graph



VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\ProgramData\SDgswYXSvL
C:\ProgramData\SDgswYXSvL\1b74a89596
\Device\KsecDD
C:\Windows\notepad.exe
C:\ProgramData\SDgswYXSvL\readme.exe:Zone.Identifier
C:\ProgramData\SDgswYXSvL\readme.exe
C:\ProgramData
C:\Windows\sysnative\WSHTCPIP.DLL
C:\Windows\sysnative\wship6.dll
C:\Windows\sysnative\wshqos.dll
C:\ProgramData\SDgswYXSvL\cfgi
C:\ProgramData\SDgswYXSvL\cfg
C:\Windows\sysnative\tzres.dll

RESOLVED APIS

kernel32.dll.IsWow64Process
ntdll.dll.RtlGetVersion
shell32.dll.SHGetKnownFolderPath
rasapi32.dll.RasConnectionNotificationW
sechost.dll.NotifyServiceStatusChangeA
cryptbase.dll.SystemFunction036
ole32.dll.CoInitializeEx
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
ole32.dll.CoUninitialize
oleaut32.dll.#500
kernel32.dll.AddVectoredExceptionHandler
kernel32.dll.AssignProcessToJobObject
kernel32.dll.CancelIo
kernel32.dll.CloseHandle
kernel32.dll.ConnectNamedPipe
kernel32.dll.CopyFileW
kernel32.dll.CreateDirectoryW

kernel32.dll.CreateEventA
kernel32.dll.CreateFileA
kernel32.dll.CreateFileW
kernel32.dll.CreateHardLinkW
kernel32.dll.CreateIoCompletionPort
kernel32.dll.CreateJobObjectW
kernel32.dll.CreateNamedPipeA
kernel32.dll.CreateNamedPipeW
kernel32.dll.CreateProcessW
kernel32.dll.CreateSemaphoreA
kernel32.dll.CreateSemaphoreW
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.DebugBreak
kernel32.dll.DeleteCriticalSection
kernel32.dll.DeviceIoControl
kernel32.dll.DuplicateHandle
kernel32.dll.EnterCriticalSection
kernel32.dll.FileTimeToSystemTime
kernel32.dll.FillConsoleOutputAttribute
kernel32.dll.FillConsoleOutputCharacterW
kernel32.dll.FlushFileBuffers
kernel32.dll.FormatMessageA
kernel32.dll.FreeConsole
kernel32.dll.GetConsoleCursorInfo
kernel32.dll.GetConsoleMode
kernel32.dll.GetConsoleScreenBufferInfo
kernel32.dll.GetConsoleTitleW
kernel32.dll.GetConsoleWindow
kernel32.dll.GetCurrentDirectoryW
kernel32.dll.GetCurrentProcess
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetCurrentThread
kernel32.dll.GetCurrentThreadId
kernel32.dll.GetEnvironmentVariableW
kernel32.dll.GetExitCodeProcess

kernel32.dll.GetFileAttributesW
kernel32.dll.GetFileInformationByHandle
kernel32.dll.GetFileType
kernel32.dll.GetHandleInformation
kernel32.dll.GetLastError
kernel32.dll.GetLongPathNameW
kernel32.dll.GetModuleFileNameW
kernel32.dll.GetModuleHandleA
kernel32.dll.GetModuleHandleW
kernel32.dll.GetNamedPipeHandleStateA
kernel32.dll.GetNumberOfConsoleInputEvents
kernel32.dll.GetProcAddress
kernel32.dll.GetProcessAffinityMask
kernel32.dll.GetProcessIoCounters
kernel32.dll.GetProcessTimes
kernel32.dll.GetQueuedCompletionStatus
kernel32.dll.GetShortPathNameW
kernel32.dll.GetStartupInfoA
kernel32.dll.GetStartupInfoW
kernel32.dll.GetStdHandle
kernel32.dll.GetSystemInfo
kernel32.dll.GetSystemTimeAdjustment
kernel32.dll.GetSystemTimeAsFileTime

EXECUTED COMMANDS

"C:\Windows\notepad.exe" -c "C:\ProgramData\SDgswYXSvL\cfgi"
"C:\Windows\notepad.exe" -c "C:\ProgramData\SDgswYXSvL\cfg"

READ FILES

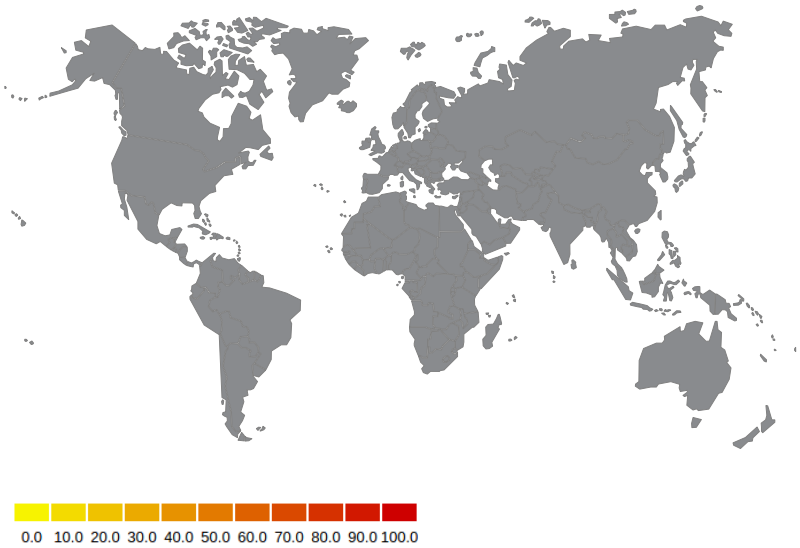
\Device\KsecDD
C:\Windows\sysnative\wship6.dll
C:\Windows\sysnative\wshqos.dll
C:\ProgramData\SDgswYXSvL\cfgi
C:\ProgramData\SDgswYXSvL\cfg
C:\Windows\sysnative\tzres.dll

MUTEXES

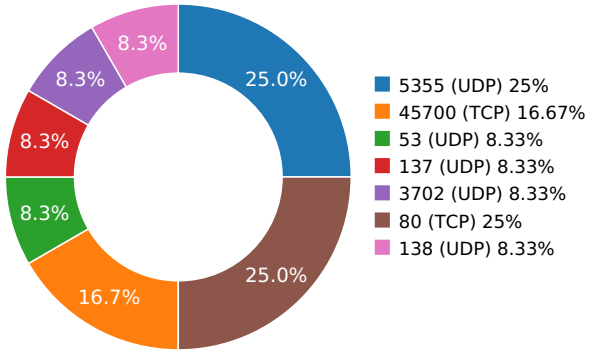
1b74a89596c952bf8c2f
IESQMMUTEX_0_208

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
xmr.pool.minergate.com	136.243.94.27	Germany	24940		Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
185.202.172.106	80	GET	1.1	WinInetGet/0.1	3	7.20315909386

Path: /file.txt
URI: http://185.202.172.106/file.txt

DNS QUERIES

Request	Type
xmr.pool.minergate.com	A

Answers
- 46.4.120.155 (A)
- 94.130.64.225 (A)
- 136.243.102.157 (A)
- 136.243.88.145 (A)
- 78.46.23.253 (A)
- 94.130.9.194 (A)
- 136.243.94.27 (A)
- 176.9.0.89 (A)
- 176.9.147.178 (A)
- 94.130.48.154 (A)

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
7.20315909386	Sandbox	185.202.172.106	80
8.62883400917	Sandbox	136.243.102.157	45700
12.4729821682	Sandbox	185.202.172.106	80
21.9156141281	Sandbox	46.4.120.155	45700

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
6.95502305031	Sandbox	224.0.0.252	5355
7.01207613945	Sandbox	224.0.0.252	5355
7.02901101112	Sandbox	192.168.56.255	137
7.04847002029	Sandbox	239.255.255.250	3702
8.4838821888	Sandbox	8.8.4.4	53
9.64455318451	Sandbox	224.0.0.252	5355
13.0894751549	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

STATIC FILE INFO

File Name:	readme.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	faf73abf89f0df908254e72c3fb02eaf0a8f5ddc
MD5:	4cbf5af84e0424aeb79910b840d893b1
First Seen Date:	2018-05-30 23:08:53.419080 (about 8 hours ago)
Number Of Clients Seen:	2
Last Analysis Date:	2018-05-30 23:08:53.419080 (about 8 hours ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	4
Trid	[]
Compilation Time Stamp	0x5B0AD662 [Sun May 27 16:01:38 2018 UTC]
Entry Point	0x403fd0 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	891392
Ssdeep	
Sha256	2a11a2028695a258986900e982fe7c19f426ef20d06ae4719c83f6e9a2f70717
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

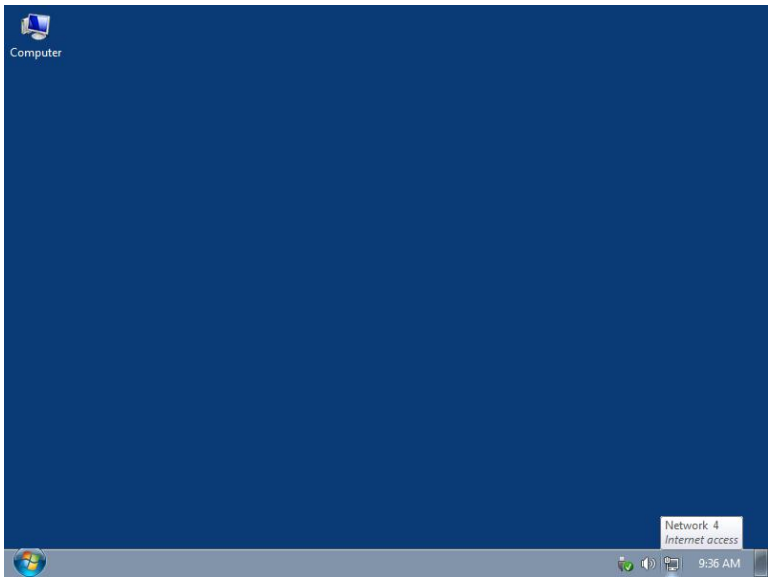
NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x6ec4	0x7000	6.18278390477	d79b02f8eb272f2846fe90f84ef22fe0
.rdata	0x8000	0x19ba	0x1a00	5.20314388738	a84e32acdaea6c17ec906ee244cec795
.data	0xa000	0xd1bb0	0xd0400	7.95860130701	cca1c85e6625b8fb704182457cbecbb0
.reloc	0xdc000	0x6a4	0x800	6.06198182474	901f7d0af48dfddf8973ce6e6e11c094

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS


Computer
9:36 AM


Computer
Network 4
Internet access
9:36 AM


Computer
9:36 AM