VALKYRIE COMODO

Summary

File Name: helponyon.info.exe

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

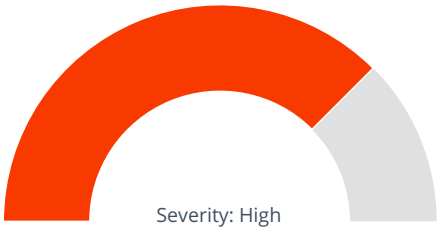
SHA1: a9f315251fdbeaa49965d86977518adbbd1d7a2c

MD5: fe296bb6c87077cd238899eb5e3d6cde

MALWARE

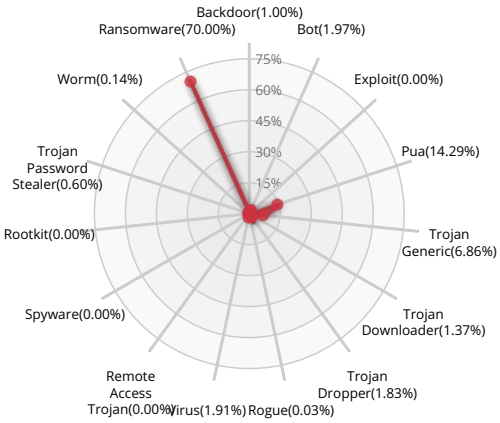
Valkyrie Final Verdict

DETECTION SECTION

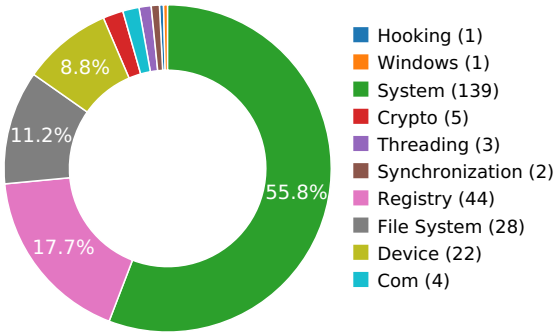


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

SPAM, UNWANTED ADVERTISEMENTS AND RANSOM DEMANDS

Writes a potential ransom message to disk Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup Show sources

VALKYRIE COMODO

Behavior Graph

19:52:05 **19:52:06** **19:52:06**

PID 2940

19:52:05 **Create Process** The malicious file created a child process as a9f315251fdbeaa49965d86977518adbbd1d7a2c.exe **(PPID 1716)**

19:52:06 RegSetValueExW

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Roaming\!#_RESTORE_FILES_#!.inf
\??\MountPointManager

READ REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation

RESOLVED APIS

kernel32.dll.InitializeCriticalSectionEx
kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.FlsGetValue
kernel32.dll.LCMapStringEx
kernel32.dll.FlsFree
kernel32.dll.InitOnceExecuteOnce
kernel32.dll.CreateEventExW
kernel32.dll.CreateSemaphoreW
kernel32.dll.CreateSemaphoreExW
kernel32.dll.CreateThreadpoolTimer
kernel32.dll.SetThreadpoolTimer
kernel32.dll.WaitForThreadpoolTimerCallbacks
kernel32.dll.CloseThreadpoolTimer
kernel32.dll.CreateThreadpoolWait
kernel32.dll.SetThreadpoolWait
kernel32.dll.CloseThreadpoolWait

kernel32.dll.FlushProcessWriteBuffers
kernel32.dll.FreeLibraryWhenCallbackReturns
kernel32.dll.GetCurrentProcessorNumber
kernel32.dll.CreateSymbolicLinkW
kernel32.dll.GetTickCount64
kernel32.dll.GetFileInformationByHandleEx
kernel32.dll.SetFileInformationByHandle
kernel32.dll.InitializeConditionVariable
kernel32.dll.WakeConditionVariable
kernel32.dll.WakeAllConditionVariable
kernel32.dll.SleepConditionVariableCS
kernel32.dll.InitializeSRWLock
kernel32.dll.AcquireSRWLockExclusive
kernel32.dll.TryAcquireSRWLockExclusive
kernel32.dll.ReleaseSRWLockExclusive
kernel32.dll.SleepConditionVariableSRW
kernel32.dll.CreateThreadpoolWork
kernel32.dll.SubmitThreadpoolWork
kernel32.dll.CloseThreadpoolWork
kernel32.dll.CompareStringEx
kernel32.dll.GetLocaleInfoEx
api-ms-win-core-synch-l1-2-0.dll.InitializeConditionVariable
api-ms-win-core-synch-l1-2-0.dll.SleepConditionVariableCS
api-ms-win-core-synch-l1-2-0.dll.WakeAllConditionVariable
kernel32.dll.AreFileApisANSI
kernel32.dll.EnumSystemLocalesEx
kernel32.dll.GetDateFormatEx
kernel32.dll.GetTimeFormatEx
kernel32.dll.GetUserDefaultLocaleName
kernel32.dll.IsValidLocaleName
kernel32.dll.LCIDToLocaleName
kernel32.dll.LocaleNameToLCID
advapi32.dll.SystemFunction036
cryptbase.dll.SystemFunction001

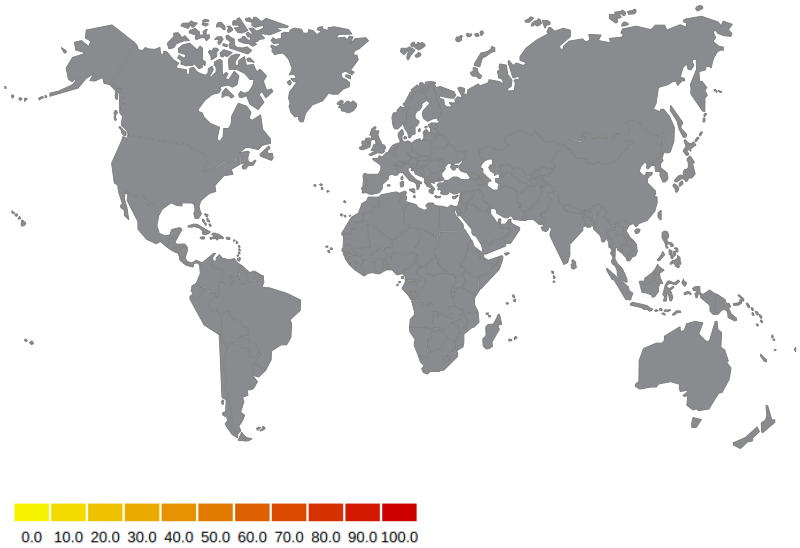
cryptbase.dll.SystemFunction002
cryptbase.dll.SystemFunction003
cryptbase.dll.SystemFunction004
cryptbase.dll.SystemFunction005
cryptbase.dll.SystemFunction028
cryptbase.dll.SystemFunction029
cryptbase.dll.SystemFunction034
cryptbase.dll.SystemFunction036
cryptbase.dll.SystemFunction040
cryptbase.dll.SystemFunction041
cryptsp.dll.CryptAcquireContextA
cryptsp.dll.CryptEncrypt
setupapi.dll.CM_Get_Device_Interface_List_Size_ExW
setupapi.dll.CM_Get_Device_Interface_List_ExW
comctl32.dll.#386

REGISTRY KEYS

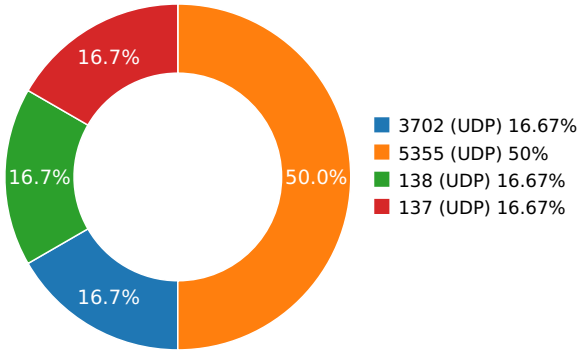
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\DECRYPTINFO
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\a9f315251fdbeaa49965d86977518adbbd1d7a2c.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.08790397644	Sandbox	224.0.0.252	5355
3.11511301994	Sandbox	224.0.0.252	5355
3.12408590317	Sandbox	239.255.255.250	3702
3.14284396172	Sandbox	192.168.56.255	137
5.67342400551	Sandbox	224.0.0.252	5355
6.15342187881	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\!#_RESTORE_FILES_#!.Inf	**Type :** ASCII text, with CRLF line terminators **MD5 :** 176304d7a51daf17cabb9d45e8d5e4ed **SHA-1 :** 6eac45ccf13524c313c715d413985c5b74a910f8 **SHA-256 :** 7f14afa7fe7dce13f3dcaee74a67475f888bbd72a **SHA-512 :** 4ea9234f65a1b8c5a1618a8ecc8db31f42c64e1f2 **Size :** 1.312 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	helponyon.info.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	a9f315251fdbeaa49965d86977518adbbd1d7a2c
MD5:	fe296bb6c87077cd238899eb5e3d6cde
First Seen Date:	2017-06-17 22:36:24.192204 (2 years ago)
Number Of Clients Seen:	4
Last Analysis Date:	2017-06-17 22:36:24.192204 (2 years 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
File Type Enum	6
Number Of Sections	5
Compilation Time Stamp	0x593FAF7A [Tue Jun 13 09:25:14 2017 UTC]
Entry Point	0x40b003 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	241664
Sha256	49470e0e56c491a0bb8483859cfdb18067047e7740bc1709835f653ffd6730ad
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x26b01	0x26c00	6.638149853	f7e7aeac5cb7af019aa970a9c43ddad9
.rdata	0x28000	0x1055c	0x10600	5.56894429188	cd2bd59e85bfd012a5532ed75f5ca6d2
.data	0x39000	0x1406da8	0x1000	3.50891721475	3b3bd3e6245638882be4959d37664126
.tls	0x1440000	0x9	0x200	0.0203931352361	1f354d76203061bfdd5a53dae48d5435
.reloc	0x1441000	0x2720	0x2800	6.57492740972	b3dea16b531d9c0e8671fb73af0c08ba

PE Imports

- KERNEL32.dll
  - GetCurrentProcessorNumber
  - ExitProcess
  - lstrcpynA
  - WinExec
  - GetTickCount
  - GetDriveTypeW
  - GetLastError
  - HeapSize
  - GetLocalTime
  - ReadConsoleW
  - WriteConsoleW
  - SetStdHandle
  - GetLogicalDrives
  - FreeEnvironmentStringsW
  - OpenMutexA
  - Sleep
  - GetCurrentThreadId
  - CreateMutexA
  - FindFirstFileA
  - FindClose
  - FindNextFileA
  - ExpandEnvironmentStringsW
  - CreateFileW
  - GetModuleFileNameA
  - GetFileTime
  - lstrcmpiA

    - SystemTimeToFileTime
    - GetFileSize
    - CloseHandle
    - FileTimeToSystemTime
    - CreateFileA
    - MoveFileExA
    - lstrlenA
    - GetEnvironmentStringsW
    - GetCommandLineW
    - GetCommandLineA
    - GetOEMCP
    - IsValidCodePage
    - FindFirstFileExA
    - GetProcessHeap
    - SetFilePointerEx
    - GetConsoleMode
    - SetFileTime
    - WriteFile
    - ReadFile
    - WideCharToMultiByte
    - EnterCriticalSection
    - LeaveCriticalSection
    - DeleteCriticalSection
    - EncodePointer
    - DecodePointer
    - MultiByteToWideChar
    - SetLastError
    - InitializeCriticalSectionAndSpinCount
    - CreateEventW
    - TlsAlloc
    - TlsGetValue
    - TlsSetValue
    - TlsFree
    - GetSystemTimeAsFileTime
    - GetModuleHandleW
    - GetProcAddress
    - LCMapStringW
    - GetLocaleInfoW
    - GetStringTypeW
    - GetCPInfo
    - UnhandledExceptionFilter
    - SetUnhandledExceptionFilter
    - GetCurrentProcess
    - TerminateProcess
    - IsProcessorFeaturePresent
    - SetEvent
    - ResetEvent
    - WaitForSingleObjectEx
    - IsDebuggerPresent
    - GetStartupInfoW
    - QueryPerformanceCounter
    - GetCurrentProcessId
    - InitializeSListHead
    - RtlUnwind
    - RaiseException
    - FreeLibrary
    - LoadLibraryExW
    - HeapAlloc
    - HeapReAlloc
    - HeapFree
    - GetModuleHandleExW
    - GetStdHandle
    - GetACP
    - IsValidLocale
    - GetUserDefaultLCID
    - EnumSystemLocalesW
    - GetFileType
    - FlushFileBuffers
    - GetConsoleCP
    - SetEndOfFile
- USER32.dll
    - GetDC
    - FillRect
    - GetSystemMetrics
    - GetActiveWindow

    - wsprintfW
    - DrawTextW
    - SystemParametersInfoW
    - wsprintfA
    - GetClipboardOwner
- GDI32.dll
    - GetDIBits
    - CreateCompatibleBitmap
    - SelectObject
    - CreateCompatibleDC
    - SetTextColor
    - SetBkMode
    - CreateSolidBrush
    - CreateFontIndirectW
- ADVAPI32.dll
    - RegOpenKeyExW
    - CryptHashData
    - CryptDeriveKey
    - RegCloseKey
    - RegSetValueExW
    - CryptSetKeyParam
    - CryptAcquireContextA
    - CryptEncrypt
    - CryptCreateHash
- SHELL32.dll
    - ShellExecuteA
    - SHGetPathFromIDListA
    - SHGetSpecialFolderLocation
    - ShellExecuteW
- SHLWAPI.dll
    - PathFindFileNameA
    - PathFindExtensionA
- MPR.dll
    - WNetEnumResourceA
    - WNetGetLastErrorA
    - WNetOpenEnumA
    - WNetCloseEnum
- CRYPT32.dll
    - CryptStringToBinaryA
    - CryptDecodeObjectEx
    - CryptImportPublicKeyInfo

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS


Computer
7:57 PM


Computer
7:57 PM


Computer
7:52 PM