VALKYRIE COMODO

Summary

File Name: Bitmin.exe

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

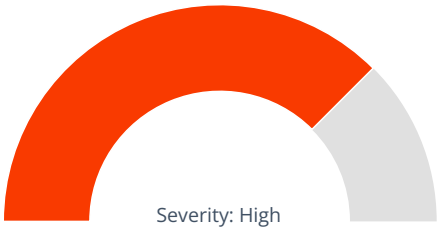
SHA1: 306cb59efe08a6a1eee2a9fd30702f5561d4413d

MD5: 18c1e0b58f3928da5d2e4ab65ad75928

MALWARE

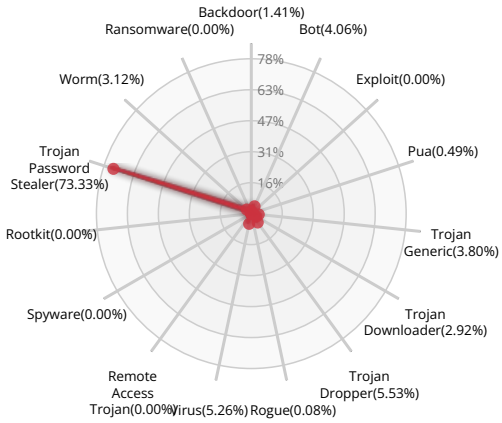
Valkyrie Final Verdict

DETECTION SECTION

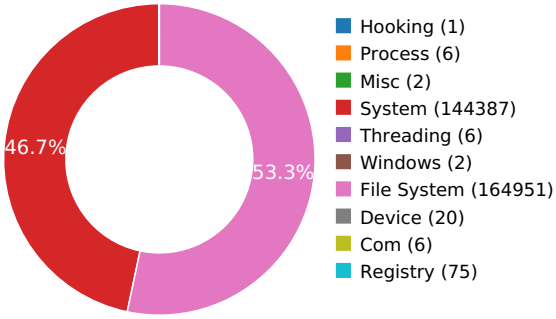


Verdict: Malware

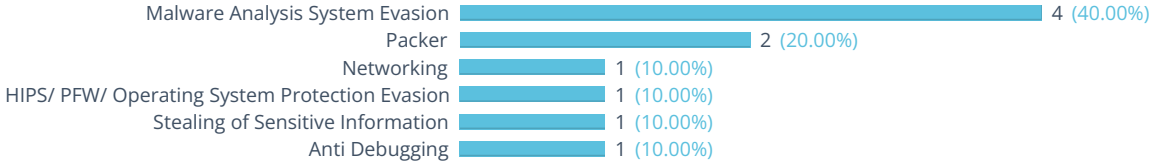
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

NETWORKING

Installs WinPCAP	Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Attempts to identify installed AV products by installation directory	Show sources

PACKER

The binary likely contains encrypted or compressed data.	Show sources
The executable is compressed using UPX	Show sources

STEALING OF SENSITIVE INFORMATION

Harvests information related to installed mail clients	Show sources

ANTI DEBUGGING

Checks for the presence of known devices from debuggers and forensic tools	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Attempts to identify installed analysis tools by a known file location	Show sources
Detects VirtualBox through the presence of a file	Show sources
Creates a hidden or system file	Show sources
Network activity detected but not expressed in API logs	

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

\Device\KsecDD
C:\Users\user\AppData\Local\Temp\
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\E813.tmp
C:\Users\user\AppData\Local\Temp\E813.tmp\1.bat
C:\Users\user\AppData\Local\Temp\E814.tmp
C:\Users\user\AppData\Local\Temp\306cb59efe08a6a1eee2a9fd30702f5561d4413d.exe
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\"C:\Users\user\AppData\Local\Temp\E813.tmp\1.bat"
A:\
A:*
B:\
B:*
C:\
C:*
C:\$Recycle.Bin
C:\$Recycle.Bin*
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000*
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000\desktop.ini
C:\Documents and Settings
C:\pagefile.sys
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui
C:\Program Files
C:\Program Files*
C:\Program Files\7-Zip
C:\Program Files\7-Zip*
C:\Program Files\7-Zip\7-zip.chm

C:\Program Files\7-Zip\7-zip.dll
C:\Program Files\7-Zip\7-zip32.dll
C:\Program Files\7-Zip\7z.dll
C:\Program Files\7-Zip\7z.exe
C:\Program Files\7-Zip\7z.sfx
C:\Program Files\7-Zip\7zCon.sfx
C:\Program Files\7-Zip\7zFM.exe
C:\Program Files\7-Zip\7zG.exe
C:\Program Files\7-Zip\descript.ion
C:\Program Files\7-Zip\History.txt
C:\Program Files\7-Zip\Lang
C:\Program Files\7-Zip\Lang*
C:\Program Files\7-Zip\Lang\af.txt
C:\Program Files\7-Zip\Lang\an.txt
C:\Program Files\7-Zip\Lang\ar.txt
C:\Program Files\7-Zip\Lang\ast.txt
C:\Program Files\7-Zip\Lang\az.txt
C:\Program Files\7-Zip\Lang\ba.txt
C:\Program Files\7-Zip\Lang\be.txt
C:\Program Files\7-Zip\Lang\bg.txt
C:\Program Files\7-Zip\Lang\bn.txt
C:\Program Files\7-Zip\Lang\br.txt
C:\Program Files\7-Zip\Lang\ca.txt
C:\Program Files\7-Zip\Lang\co.txt
C:\Program Files\7-Zip\Lang\cs.txt
C:\Program Files\7-Zip\Lang\cy.txt
C:\Program Files\7-Zip\Lang\da.txt
C:\Program Files\7-Zip\Lang\de.txt
C:\Program Files\7-Zip\Lang\el.txt
C:\Program Files\7-Zip\Lang\en.ttt
C:\Program Files\7-Zip\Lang\eo.txt
C:\Program Files\7-Zip\Lang\es.txt
C:\Program Files\7-Zip\Lang\et.txt
C:\Program Files\7-Zip\Lang\eu.txt
C:\Program Files\7-Zip\Lang\ext.txt

C:\Program Files\7-Zip\Lang\fa.txt
C:\Program Files\7-Zip\Lang\fi.txt
C:\Program Files\7-Zip\Lang\fr.txt
C:\Program Files\7-Zip\Lang\fur.txt
C:\Program Files\7-Zip\Lang\fy.txt
C:\Program Files\7-Zip\Lang\ga.txt
C:\Program Files\7-Zip\Lang\gl.txt
C:\Program Files\7-Zip\Lang\gu.txt
C:\Program Files\7-Zip\Lang\he.txt

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
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
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\PathCompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar

HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable

RESOLVED APIS

kernel32.dll.GetModuleHandleA
kernel32.dll.HeapCreate
kernel32.dll.GetCommandLineA
kernel32.dll.RemoveDirectoryA
kernel32.dll.GetTempFileNameA
kernel32.dll.GetShortPathNameA
kernel32.dll.HeapDestroy
kernel32.dll.ExitProcess
kernel32.dll.GetExitCodeProcess
kernel32.dll.FindResourceA
kernel32.dll.LoadResource
kernel32.dll.SizeofResource
kernel32.dll.HeapAlloc
kernel32.dll.HeapFree
kernel32.dll.Sleep
kernel32.dll.LoadLibraryA
kernel32.dll.GetProcAddress
kernel32.dll.FreeLibrary
kernel32.dll.GetCurrentThreadId
kernel32.dll.GetCurrentProcessId
kernel32.dll.CloseHandle
kernel32.dll.InitializeCriticalSection
kernel32.dll.GetModuleFileNameA
kernel32.dll.GetEnvironmentVariableA
kernel32.dll.SetEnvironmentVariableA
kernel32.dll.GetCurrentProcess
kernel32.dll.TerminateProcess
kernel32.dll.RtlLookupFunctionEntry

kernel32.dll.RtlVirtualUnwind
kernel32.dll.RemoveVectoredExceptionHandler
kernel32.dll.AddVectoredExceptionHandler
kernel32.dll.EnterCriticalSection
kernel32.dll.LeaveCriticalSection
kernel32.dll.GetVersionExA
kernel32.dll.HeapReAlloc
kernel32.dll.SetLastError
kernel32.dll.TlsAlloc
kernel32.dll.GetCurrentDirectoryA
kernel32.dll.SetCurrentDirectoryA
kernel32.dll.GetTempPathA
kernel32.dll.SetFileAttributesA
kernel32.dll.DeleteFileA
kernel32.dll.CreateDirectoryA
kernel32.dll.WriteFile
kernel32.dll.CreateFileA
kernel32.dll.SetFilePointer
kernel32.dll.ReadFile
kernel32.dll.DeleteCriticalSection
comctl32.dll.InitCommonControlsEx
gdi32.dll.GetStockObject
gdi32.dll.SelectObject
gdi32.dll.SetTextColor
gdi32.dll.SetBkColor
gdi32.dll.GetTextExtentPoint32A
gdi32.dll.CreateSolidBrush
gdi32.dll.DeleteObject
gdi32.dll.GetObjectA
gdi32.dll.CreateCompatibleDC
gdi32.dll.GetDIBits
gdi32.dll.DeleteDC
gdi32.dll.GetObjectType
gdi32.dll.CreateDIBSection
gdi32.dll.BitBlt

gdi32.dll.CreateBitmap
gdi32.dll.SetPixel
msvcrt.dll.memset
msvcrt.dll.memcpy
msvcrt.dll.strncmp
msvcrt.dll.memmove
msvcrt.dll.strncpy
msvcrt.dll._strnicmp
msvcrt.dll.strlen
msvcrt.dll.strcmp
msvcrt.dll.sprintf
msvcrt.dll.fabs
msvcrt.dll.ceil

DELETED FILES

C:\Users\user\AppData\Local\Temp\E813.tmp
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000\desktop.ini
C:\$Recycle.Bin\S-1-5-21-2298303332-66077612-2598613238-1000
C:\$Recycle.Bin
C:\Documents and Settings
C:\pagefile.sys
C:\Program Files\7-Zip\7-zip.chm
C:\Program Files\7-Zip\7-zip.dll
C:\Program Files\7-Zip\7-zip32.dll
C:\Program Files\7-Zip\7z.dll
C:\Program Files\7-Zip\7z.exe
C:\Program Files\7-Zip\7z.sfx
C:\Program Files\7-Zip\7zCon.sfx
C:\Program Files\7-Zip\7zFM.exe
C:\Program Files\7-Zip\7zG.exe
C:\Program Files\7-Zip\descript.ion
C:\Program Files\7-Zip\History.txt
C:\Program Files\7-Zip\Lang\af.txt
C:\Program Files\7-Zip\Lang\an.txt
C:\Program Files\7-Zip\Lang\ar.txt

C:\Program Files\7-Zip\Lang\ast.txt

C:\Program Files\7-Zip\Lang\az.txt

C:\Program Files\7-Zip\Lang\ba.txt

C:\Program Files\7-Zip\Lang\be.txt

C:\Program Files\7-Zip\Lang\bg.txt

C:\Program Files\7-Zip\Lang\bn.txt

C:\Program Files\7-Zip\Lang\br.txt

C:\Program Files\7-Zip\Lang\ca.txt

C:\Program Files\7-Zip\Lang\co.txt

C:\Program Files\7-Zip\Lang\cs.txt

C:\Program Files\7-Zip\Lang\cy.txt

C:\Program Files\7-Zip\Lang\da.txt

C:\Program Files\7-Zip\Lang\de.txt

C:\Program Files\7-Zip\Lang\el.txt

C:\Program Files\7-Zip\Lang\en.ttt

C:\Program Files\7-Zip\Lang\eo.txt

C:\Program Files\7-Zip\Lang\es.txt

C:\Program Files\7-Zip\Lang\et.txt

C:\Program Files\7-Zip\Lang\eu.txt

C:\Program Files\7-Zip\Lang\ext.txt

C:\Program Files\7-Zip\Lang\fa.txt

C:\Program Files\7-Zip\Lang\fi.txt

C:\Program Files\7-Zip\Lang\fr.txt

C:\Program Files\7-Zip\Lang\fur.txt

C:\Program Files\7-Zip\Lang\fy.txt

C:\Program Files\7-Zip\Lang\ga.txt

C:\Program Files\7-Zip\Lang\gl.txt

C:\Program Files\7-Zip\Lang\gu.txt

C:\Program Files\7-Zip\Lang\he.txt

C:\Program Files\7-Zip\Lang\hi.txt

C:\Program Files\7-Zip\Lang\hr.txt

C:\Program Files\7-Zip\Lang\hu.txt

C:\Program Files\7-Zip\Lang\hy.txt

C:\Program Files\7-Zip\Lang\id.txt

C:\Program Files\7-Zip\Lang\io.txt

C:\Program Files\7-Zip\Lang\is.txt
C:\Program Files\7-Zip\Lang\it.txt
C:\Program Files\7-Zip\Lang\ja.txt
C:\Program Files\7-Zip\Lang\ka.txt
C:\Program Files\7-Zip\Lang\kaa.txt
C:\Program Files\7-Zip\Lang\kk.txt
C:\Program Files\7-Zip\Lang\ko.txt
C:\Program Files\7-Zip\Lang\ku-ckb.txt
C:\Program Files\7-Zip\Lang\ku.txt
C:\Program Files\7-Zip\Lang\ky.txt
C:\Program Files\7-Zip\Lang\lij.txt
C:\Program Files\7-Zip\Lang\lt.txt
C:\Program Files\7-Zip\Lang\lv.txt
C:\Program Files\7-Zip\Lang\mk.txt
C:\Program Files\7-Zip\Lang\mn.txt
C:\Program Files\7-Zip\Lang\mng.txt
C:\Program Files\7-Zip\Lang\mng2.txt
C:\Program Files\7-Zip\Lang\mr.txt
C:\Program Files\7-Zip\Lang\ms.txt
C:\Program Files\7-Zip\Lang\nb.txt
C:\Program Files\7-Zip\Lang\ne.txt

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
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
HKEY_CURRENT_USER\Software\Policies\Microsoft\Windows\System
HKEY_LOCAL_MACHINE\Software\Microsoft\Command Processor
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\DisableUNCCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\EnableExtensions
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\DelayedExpansion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\DefaultColor
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\CompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\PathCompletionChar
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Command Processor\AutoRun
HKEY_CURRENT_USER\Software\Microsoft\Command Processor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DisableUNCCheck
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\EnableExtensions
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DelayedExpansion
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\DefaultColor
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\CompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\PathCompletionChar
HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SafeBoot\Option
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Windows Error Reporting\WMR\Disable

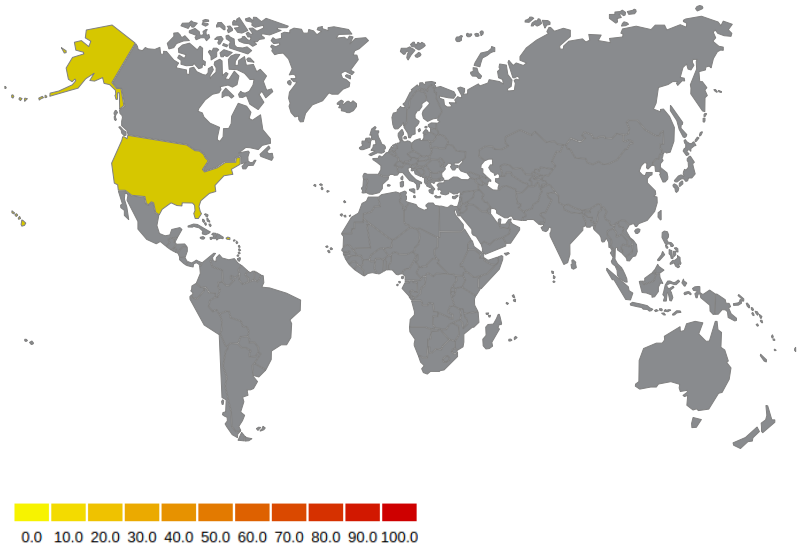
READ FILES

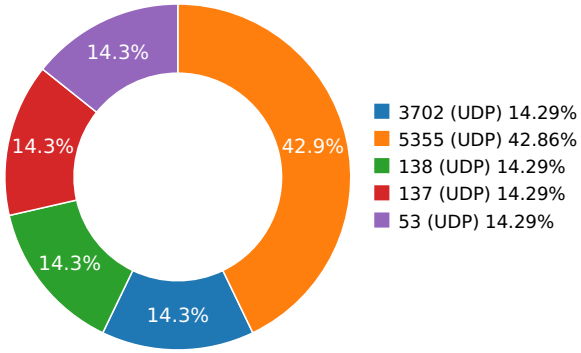
\Device\KsecDD

C:\Users\user\AppData\Local\Temp\E813.tmp
C:\Users\user\AppData\Local\Temp\E813.tmp\1.bat
C:\Users\user\AppData\Local\Temp\E814.tmp
C:\Windows\sysnative\en-US\KERNELBASE.dll.mui

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

DNS QUERIES

Request	Type
teredo.ipv6.microsoft.com	A
Answers - (NXDOMAIN)	

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.19669413567	Sandbox	224.0.0.252	5355
3.21530413628	Sandbox	224.0.0.252	5355
3.22122597694	Sandbox	239.255.255.250	3702
3.2655479908	Sandbox	192.168.56.255	137
5.77494096756	Sandbox	224.0.0.252	5355
9.26572299004	Sandbox	192.168.56.255	138
109.526139975	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\E813.Tmp\1.Bat	**Type :** ASCII text, with CRLF line terminators **MD5 :** 25ac6edca724adb1de8e1872bd2055a1 **SHA-1 :** 6360beff8c1c1fad02c4ea0d1df824c5b65de3b5 **SHA-256 :** cdbe9eb89fe4d442a8b9231cd7ef2ead1dddbedf **SHA-512 :** 44107f48f32d250d0887f78e346ee9bf0c219632(**Size :** 0.967 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	Bitmin.exe
File Type:	PE32+ executable (GUI) x86-64, for MS Windows
SHA1:	306cb59efe08a6a1eee2a9fd30702f5561d4413d
MD5:	18c1e0b58f3928da5d2e4ab65ad75928
First Seen Date:	2018-03-10 07:29:32.769349 (8 years ago)
Number Of Clients Seen:	1
Last Analysis Date:	2018-03-10 07:29:32.769349 (8 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

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	[[87.0, u'UPX compressed Win32 Executable'], [6.4, u'Generic Win/DOS Executable'], [6.4, u'DOS Executable Generic'], [0.0, u'VXD Driver']]
Compilation Time Stamp	0x55C718C5 [Sun Aug 9 09:09:25 2015 UTC]
ProductVersion	1.0.0.0
FileVersion	1,0,0,0
CompanyName	Google
Translation	0x0000 0x04e4
Entry Point	0x14002d9e0 (UPX1)
Machine Type	AMD64 only, not Itaniums, with 0200 - 64 bit
File Size	123904
Ssdeep	3072:AfrhE4kfkD0YOi2m+Swsbu2ZLQ/3AyPsAjqllnZ3:ASNYOuisa2uQO/qll
Sha256	188e8b2b92225a29007084d6e556ceb0f52c83052d2a1a1c3d474f0b97f38139
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/0/6/c/306cb59efe08a6a1eee2a9fd30702f5561d4413d', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2018:03:10 07:28:54+00:00', u'EXE:InitializedDataSize': 0, u'File:FileModifyDate': u'2018:03:10 07:28:54+00:00', u'EXE:FileVersionNumber': u'1.0.0.0', u'EXE:FileVersion': u'1,0,0,0', u'File:FileSize': u'121 kB', u'EXE:CharacterSet': u'Windows, Latin1', u'EXE:MachineType': u'AMD AMD64', u'EXE:FileOS': u'Windows 16-bit', u'EXE:ProductVersion': u'1.0.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win64 EXE', u'EXE:CompanyName': u'Google', u'File:FileName': u'306cb59efe08a6a1eee2a9fd30702f5561d4413d', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32+', u'EXE:TimeStamp': u'2015:08:09 09:09:25+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LinkerVersion': 11.5, u'EXE:FileFlags': u'Debug, Pre-release, Private build', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/3/0/6/c', u'EXE:EntryPoint': u'0x2d9e0', u'EXE:SubsystemVersion': 5.2, u'EXE:CodeSize': 32768, u'File:FileInodeChangeDate': u'2018:03:10 07:28:54+00:00', u'EXE:UninitializedDataSize': 151552, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	7045005ef4130348fa4cbfc30a6f9d04

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x25000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0x26000	0x9000	0x8600	7.96229553476	021921cf7043dadad2c4a5d73dd0fd93
.rsrc	0x2f000	0x16000	0x15c00	6.41142955367	03cc2f593639536872877021b450b73c

PE Imports

- KERNEL32.DLL
  - LoadLibraryA
  - GetProcAddress
  - VirtualProtect
  - VirtualAlloc
  - VirtualFree
  - ExitProcess
- COMCTL32.DLL
  - InitCommonControlsEx
- GDI32.DLL
  - BitBlt
- msvcrt.dll
  - fabs
- OLE32.DLL
  - CoInitialize
- SHELL32.DLL
  - ShellExecuteExA
- SHLWAPI.DLL
  - PathGetArgsA
- USER32.DLL
  - GetDC
- WINMM.DLL
  - timeBeginPeriod

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 193292, u'sha256': u'fdfeaefa06b30fc03904a9258f478cc648d5c15213d3f83a5a559c2a30c86406', u'type': u'data', u'size': 67624}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 260920, u'sha256': u'fe7165cb826bb7a858ca79232c8ad534c94bd8ed665e12675a518dc4de175064', u'type': u'dBase IV DBT of `.DBF, block length 9216, next free block index 40, next free block 4281337347, next used block 4281402883', u'size': 9640}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 270564, u'sha256': u'6af663a7628cf4c54cc436e1017509b45f9ad640797a2379fd209ebde8a5ac69', u'type': u'dBase IV DBT of @.DBF, block length 4096, next free block index 40, next free block 4279042560, next used block 4279436290', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 274832, u'sha256': u'96364051df98d5ee06441c98b379f834866e4307b8d79a6e69c9e3101ad58d04', u'type': u'dBase IV DBT of @.DBF, block length 1024, next free block index 40, next free block 11302468, next used block 10721691', u'size': 2216}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 277052, u'sha256': u'6be8ded71d601752e266498bb612497bf454741bd3547ada6d8704f72cd30484', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 278184, u'sha256': u'af32908841bc8f4e35437a1da2a890ffc648bc97b5452b990dcff495b4f332c2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 177144, u'sha256': u'6909efbde9b7592299afbc7127abb92e876917de6c1875f478aeb6c8148ceb85', u'type': u'data', u'size': 954}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 178100, u'sha256': u'325fffc2184f90a21b2d6def74cdd59458f56d63c3c7e23b57a6d7514267eca6', u'type': u'data', u'size': 14}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 178116, u'sha256': u'3c7a8111ab483de3cd024649bddac29d98547406cf7eacfa95da5e3fdc360de0', u'type': u'data', u'size': 12}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 178128, u'sha256': u'd91cf1e4aee71506f67466c3fed72c6720d7de45f27fda68f4d824ced0717a17', u'type': u'ISO-8859 text, with no line terminators', u'size': 6}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 279572, u'sha256': u'f2e2df0d9e9eaa9dfe00fd0320a551b542e1bab2d8c2a08349d8dda4fa2591e1', u'type': u'MS Windows icon resource - 6 icons, 128x128', u'size': 90}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_VERSION', u'offset': 279668, u'sha256': u'9f4e29f60d4a371ea7c33c2227b94bc3b834571bb9f5525ca268e6f427bbf92e', u'type': u'data', u'size': 368}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 280040, u'sha256': u'cbb90bd969933f7ddfe27fad7c3649f1f1bdaf2ffcaa1ffc4eb7a96376bd49c8', u'type': u'XML 1.0 document, ASCII text, with very long lines, with no line terminators', u'size': 668}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS