VALKYRIE COMODO

Summary

File Name: 2023-03-01_8efccd45c79b053ace1c9691a3add9da_mafia

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

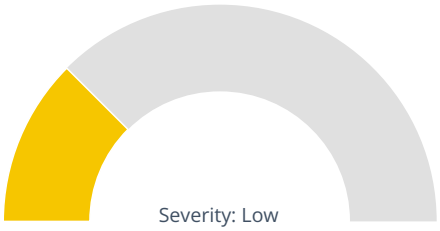
SHA1: 40f40a99ea7be53397a801921abbd77a1f9abc64

MD5: 8efccd45c79b053ace1c9691a3add9da

PUA

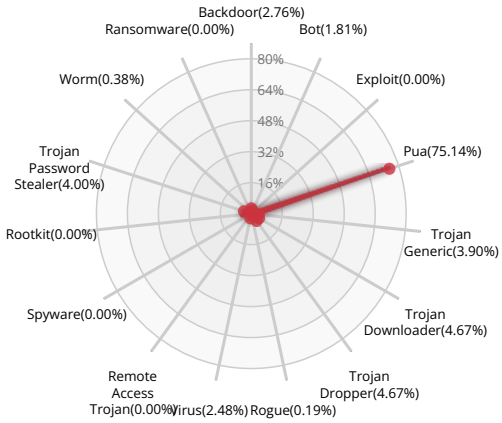
Valkyrie Final Verdict

DETECTION SECTION

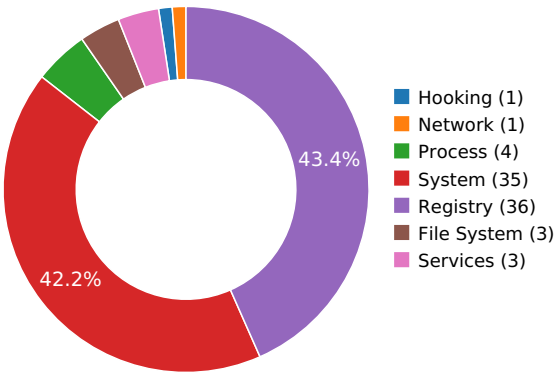


Verdict: PUA

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Data Obfuscation 1 (100.00%)

VALKYRIE COMODO

Activity Details

DATA OBFUSCATION

Unconventionial binary language: Russian

VALKYRIE COMODO

Behavior Graph

09:49:00 **09:49:00** **09:49:00**

PID 2332

09:49:00	Create Process	The malicious file created a child process as 40f40a99ea7be53397a801921abbd77a1f9abc64.exe **(PPID 2284)**

VALKYRIE COMODO

Behavior Summary

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tag
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\GroupOrderList\PNP_TDI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\tdx\Tag
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.QueryFullProcessImageNameW
kernel32.dll.QueryFullProcessImageNameA
wtsapi32.dll.WTSQuerySessionInformationA
wtsapi32.dll.WTSQuerySessionInformationW
wtsapi32.dll.WTSFreeMemory

REGISTRY KEYS

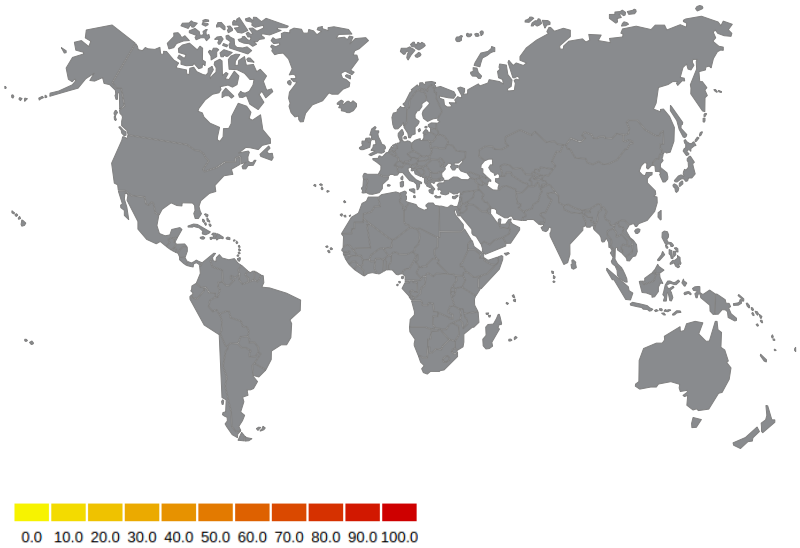
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tag
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\GroupOrderList
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\GroupOrderList\PNP_TDI
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tdx
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\tdx\Tag
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TCPIP6\Parameters\DisabledComponents
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

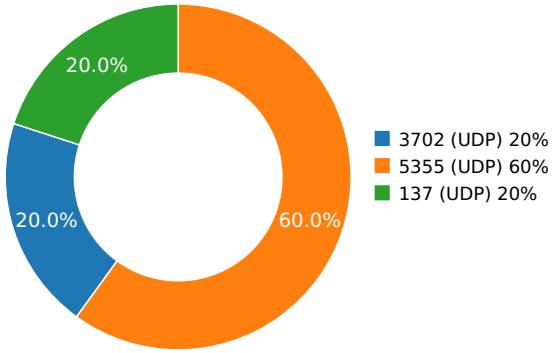
MODIFIED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Tag
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\GroupOrderList\PNP_TDI
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\TCPIP6\Parameters\DisabledComponents

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
3.08403801918	Sandbox	224.0.0.252	5355
3.10005903244	Sandbox	224.0.0.252	5355
3.10824394226	Sandbox	239.255.255.250	3702
3.1226708889	Sandbox	192.168.56.255	137
5.68672895432	Sandbox	224.0.0.252	5355

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	2023-03-01_8efccd45c79b053ace1c9691a3add9da_mafia
File Type:	PE32 executable (console) Intel 80386, for MS Windows
SHA1:	40f40a99ea7be53397a801921abbd77a1f9abc64
MD5:	8efccd45c79b053ace1c9691a3add9da
First Seen Date:	2023-03-15 13:27:27.798331 (about 5 hours ago)
Number Of Clients Seen:	2
Last Analysis Date:	2023-03-15 13:27:27.798331 (about 5 hours ago)
Human Expert Analysis Date:	2023-03-15 18:42:34.626964 (less than a minute ago)
Human Expert Analysis Result:	PUA

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	1
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[[42.2, u'Win32 Executable MS Visual C++ (generic)'], [37.3, u'Win64 Executable (generic)'], [8.8, u'Win32 Dynamic Link Library (generic)'], [6.0, u'Win32 Executable (generic)'], [2.7, u'Generic Win/DOS Executable']]
Compilation Time Stamp	0x54796616 [Sat Nov 29 06:22:14 2014 UTC]
LegalCopyright	
InternalName	
FileVersion	1, 1, 1, 0
CompanyName	
ProductName	
ProductVersion	1, 1, 1, 0
FileDescription	
OriginalFilename	
Translation	0x0419 0x04b0
Entry Point	0x4213ae (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	296224
Ssdeep	6144:Jk0tnURexVtDLJJtYd1RSWRotvcTB5E8Gl:60tnUReNDLJJtYd1RSWRotvcTr+l
Sha256	c431e7f789b17dd9879f02e4559dd713bad6eb4958f8be64f0d5da822199ac9d
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/4/0/f/4/40f40a99ea7be53397a801921abbd77a1f9abc64', u'EXE:OriginalFileName': u'', u'EXE:ProductName': u'', u'EXE:InternalName': u'', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:03:15 13:26:46+00:00', u'EXE:InitializedDataSize': 73216, u'File:FileModifyDate': u'2023:03:15 13:26:46+00:00', u'EXE:FileVersionNumber': u'1.1.1.0', u'EXE:FileVersion': u'1, 1, 1, 0', u'File:FileSize': u'289 kB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Win32', u'EXE:ProductVersion': u'1, 1, 1, 0', u'EXE:ObjectFileType': u'Dynamic link library', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'', u'File:FileName': u'40f40a99ea7be53397a801921abbd77a1f9abc64', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.1, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2014:11:29 06:22:14+00:00', u'EXE:FileFlagsMask': u'0x0017', u'EXE:LegalCopyright': u'', u'EXE:LinkerVersion': 10.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows command line', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/4/0/f/4', u'EXE:FileDescription': u'', u'EXE:EntryPoint': u'0x213ae', u'EXE:SubsystemVersion': 5.1, u'EXE:CodeSize': 215552, u'File:FileInodeChangeDate': u'2023:03:15 13:26:46+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'Russian', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.1.1.0'}]
Mime Type	application/x-dosexec
Imphash	5a3059a8a0dd70a76ef776580685cce4

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x348b8	0x34a00	6.63336789556	a1dcf00bbf8b14fc9022bb4cd0ec7230
.rdata	0x36000	0xc2c4	0xc400	5.62897350206	ceda9ce3257cebbc57b99900ab5bf110
.data	0x43000	0x4464	0x1c00	4.09340365582	b3cb1fc94b3468c188c7e2607ad25dc6
.rsrc	0x48000	0x440	0x600	4.58177873263	a23f62b767b4ef51cee21c493e7fe22e
.reloc	0x49000	0x379e	0x3800	5.55165767203	35181fccdf47c0ee939cf6803697ca89

PE Imports

- KERNEL32.dll
  - ReadFile
  - GetOverlappedResult
  - GetLastError
  - GetProcAddress
  - ResetEvent
  - DeviceIoControl
  - WaitForMultipleObjects
  - GetModuleHandleA
  - CancelIo
  - GetCurrentProcessId
  - CreateEventA
  - GetFileSize
  - SetFilePointer
  - SetEndOfFile
  - CreateFileW
  - GetTempFileNameW
  - GetTempPathW
  - CreateDirectoryW
  - FreeLibrary
  - LoadLibraryA
  - ProcessIdToSessionId
  - OpenProcess
  - WriteFile
  - GetTickCount
  - SetEvent
  - WaitForSingleObject
  - DeleteCriticalSection
  - EnterCriticalSection
  - LeaveCriticalSection
  - InitializeCriticalSection
  - CloseHandle
  - CreateToolhelp32Snapshot
  - SetConsoleCtrlHandler
  - Process32Next
  - Sleep
  - Process32First
  - CreateFileA
  - ExitProcess
  - WriteConsoleW
  - SetStdHandle
  - LoadLibraryW
  - GetStringTypeW
  - IsValidLocale
  - EnumSystemLocalesA
  - GetLocaleInfoA
  - GetUserDefaultLCID
  - InterlockedIncrement
  - InterlockedDecrement
  - EncodePointer
  - DecodePointer
  - HeapFree
  - DeleteFileA
  - GetSystemTimeAsFileTime
  - HeapAlloc

    - ExitThread
    - GetCurrentThreadId
    - CreateThread
    - HeapReAlloc
    - GetCommandLineA
    - HeapSetInformation
    - RaiseException
    - RtlUnwind
    - WideCharToMultiByte
    - LCMapStringW
    - MultiByteToWideChar
    - GetCPInfo
    - TerminateProcess
    - GetCurrentProcess
    - UnhandledExceptionFilter
    - SetUnhandledExceptionFilter
    - IsDebuggerPresent
    - SetHandleCount
    - GetStdHandle
    - InitializeCriticalSectionAndSpinCount
    - GetFileType
    - GetStartupInfoW
    - IsProcessorFeaturePresent
    - HeapCreate
    - GetModuleHandleW
    - GetConsoleCP
    - GetConsoleMode
    - FlushFileBuffers
    - TlsAlloc
    - TlsGetValue
    - TlsSetValue
    - TlsFree
    - SetLastError
    - GetModuleFileNameW
    - GetACP
    - GetOEMCP
    - IsValidCodePage
    - GetLocaleInfoW
    - HeapSize
    - GetModuleFileNameA
    - FreeEnvironmentStringsW
    - GetEnvironmentStringsW
    - QueryPerformanceCounter
    - GetProcessHeap
- ADVAPI32.dll
    - LookupAccountSidA
    - GetTokenInformation
    - RegCloseKey
    - OpenSCManagerA
    - RegOpenKeyExA
    - StartServiceA
    - CreateServiceA
    - RegQueryValueExA
    - RegSetValueExA
    - DeleteService
    - CloseServiceHandle
    - OpenServiceA
    - AdjustTokenPrivileges
    - LookupPrivilegeValueA
    - OpenProcessToken
    - LookupAccountSidW
- PSAPI.DLL
    - GetModuleFileNameExA
- WS2_32.dll
    - WSAAddressToStringA
    - WSACleanup
    - WSAStartup
    - htons

PE Exports

?STObject_create@StLibs@@YAPAVSTObject@1@HH@Z
?pf_addFilter@StLibs@@YAH_KW4_ST_FilterType@1@KW4_ST_OpTarget@1@1@Z
?pf_canDisableFiltering@StLibs@@YAH_K@Z
?pf_deleteFilter@StLibs@@YAH_KW4_ST_FilterType@1@@Z

?pf_free@StLibs@@YAXXZ
?pf_getFilterCount@StLibs@@YAH_K@Z
?pf_getNFEventHandler@StLibs@@YAPAVNF_EventHandler@stapi@@XZ
?pf_getProcessOwnerA@StLibs@@YAHKPADH@Z
?pf_getProcessOwnerW@StLibs@@YAHKPA_WH@Z
?pf_init@StLibs@@YAHPAVSTEvents@1@PB_W@Z
?pf_isFilterActive@StLibs@@YAH_KW4_ST_FilterType@1@@Z
?pf_postObject@StLibs@@YAH_KPAVSTObject@1@@Z
?pf_setRootSSLCertSubject@StLibs@@YAXPBD@Z
?pf_unzipStream@StLibs@@YAHPAVSTStream@1@@Z

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 295104, u'sha256': u'f51bc859449969a35d7d791d843e2e34075f328ddfc41e20be33e5fac70c9282', u'type': u'data', u'size': 548}
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 295652, u'sha256': u'49a60be4b95b6d30da355a0c124af82b35000bce8f24f957d1c09ead47544a1e', u'type': u'ASCII text, with CRLF line terminators', u'size': 346}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS