VALKYRIE COMODO

# Summary

**File Name:** 49b7a7484c716ac86421602641bbab7b66a56d52

**File Type:** PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed

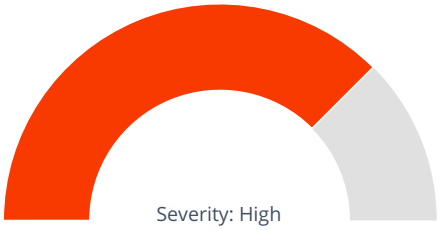
**SHA1:** 49b7a7484c716ac86421602641bbab7b66a56d52

**MD5:** a9602a5006474edb62e4b7a5f38cbf45

MALWARE

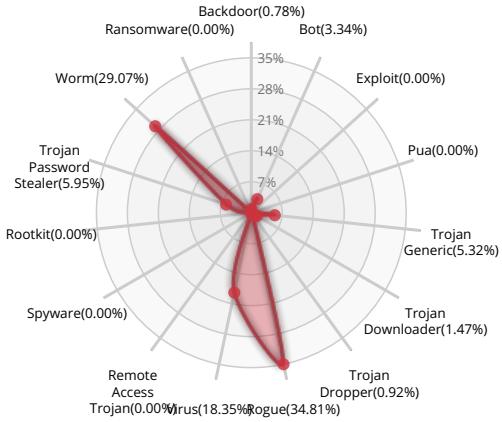
Valkyrie Final Verdict

## DETECTION SECTION

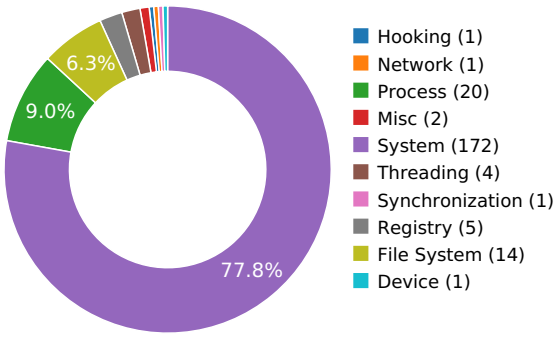



Verdict: Malware

## CLASSIFICATION




## HIGH LEVEL BEHAVIOR DISTRIBUTION




## ACTIVITY OVERVIEW

Packer 2 (100.00%)

VALKYRIE COMODO

## Activity Details

### PACKER

The binary likely contains encrypted or compressed data. Show sources

The executable is compressed using UPX Show sources

VALKYRIE COMODO

## Behavior Graph

**00:33:45** **00:33:45** **00:33:45**

**PID 2392**

| 00:33:45 | Create Process | The malicious file created a child process as 49b7a7484c716ac86421602641bbab7b66a56d52.exe **(PPID 2344)** |
|---|---|---|

# Behavior Summary

## ACCESSED FILES

| |
|---|
| \Device\KsecDD |
| C:\Windows\System32\WSHTCPIP.DLL |
| C:\Windows\System32\wship6.dll |
| C:\Windows\System32\wshqos.dll |
| C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui |
| C:\Windows\System32\tzres.dll |

## READ REGISTRY KEYS

| |
|---|
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles |

## RESOLVED APIS

| |
|---|
| kernel32.dll.WriteFile |
| kernel32.dll.WriteConsoleW |
| kernel32.dll.WaitForSingleObject |
| kernel32.dll.VirtualQuery |
| kernel32.dll.VirtualFree |
| kernel32.dll.VirtualAlloc |
| kernel32.dll.SwitchToThread |
| kernel32.dll.SetWaitableTimer |
| kernel32.dll.SetUnhandledExceptionFilter |
| kernel32.dll.SetProcessPriorityBoost |
| kernel32.dll.SetEvent |
| kernel32.dll.SetErrorMode |
| kernel32.dll.SetConsoleCtrlHandler |
| kernel32.dll.LoadLibraryA |
| kernel32.dll.LoadLibraryW |
| kernel32.dll.GetSystemInfo |
| kernel32.dll.GetSystemDirectoryA |
| kernel32.dll.GetStdHandle |
| kernel32.dll.GetQueuedCompletionStatus |
| kernel32.dll.GetProcessAffinityMask |
| kernel32.dll.GetProcAddress |

| |
|---|
| kernel32.dll.GetEnvironmentStringsW |
| kernel32.dll.GetConsoleMode |
| kernel32.dll.FreeEnvironmentStringsW |
| kernel32.dll.ExitProcess |
| kernel32.dll.DuplicateHandle |
| kernel32.dll.CreateThread |
| kernel32.dll.CreateIoCompletionPort |
| kernel32.dll.CreateEventA |
| kernel32.dll.CloseHandle |
| kernel32.dll.AddVectoredExceptionHandler |
| kernel32.dll.AddVectoredContinueHandler |
| kernel32.dll.GetQueuedCompletionStatusEx |
| kernel32.dll.LoadLibraryExA |
| kernel32.dll.LoadLibraryExW |
| advapi32.dll.SystemFunction036 |
| ntdll.dll.NtWaitForSingleObject |
| winmm.dll.timeBeginPeriod |
| winmm.dll.timeEndPeriod |
| ws2_32.dll.WSAGetOverlappedResult |
| 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 |
| kernel32.dll.SetHandleInformation |
| kernel32.dll.GetSystemDirectoryW |
| ws2_32.dll.WSAStartup |
| kernel32.dll.CancelIoEx |
| kernel32.dll.SetFileCompletionNotificationModes |

| |
|---|
| ws2_32.dll.WSAEnumProtocolsW |
| kernel32.dll.GetCommandLineW |
| kernel32.dll.GetEnvironmentVariableW |
| kernel32.dll.WTSGetActiveConsoleSessionId |
| kernel32.dll.FormatMessageW |
| wtsapi32.dll.WTSQuerySessionInformationW |
| winsta.dll.WinStationQueryInformationW |
| advapi32.dll.LookupAccountSidW |
| sechost.dll.LookupAccountSidLocalW |
| advapi32.dll.CreateWellKnownSid |
| rpcrt4.dll.RpcStringBindingComposeW |
| rpcrt4.dll.RpcBindingFromStringBindingW |
| rpcrt4.dll.RpcStringFreeW |
| rpcrt4.dll.RpcBindingSetAuthInfoExW |
| sechost.dll.LookupAccountNameLocalW |
| rpcrt4.dll.NdrClientCall2 |
| rpcrt4.dll.RpcBindingFree |
| advapi32.dll.LookupAccountNameW |
| advapi32.dll.ConvertSidToStringSidW |
| kernel32.dll.LocalFree |

## REGISTRY KEYS

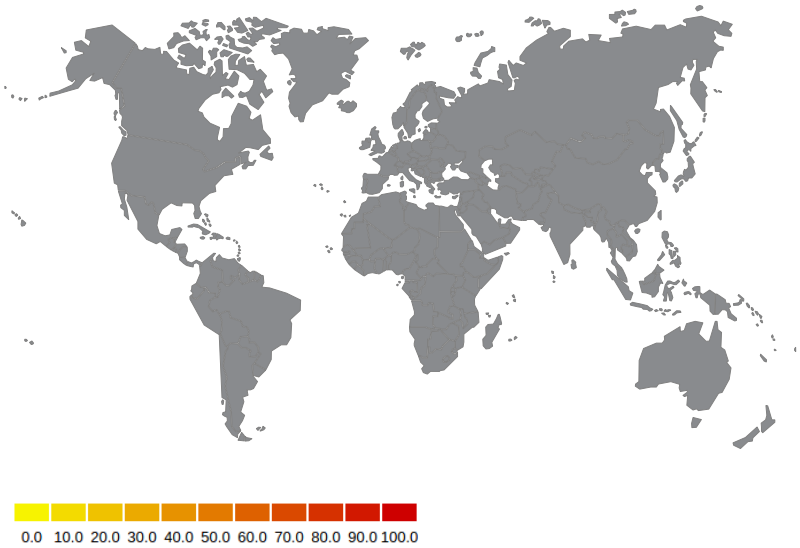
| |
|---|
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR |
| HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable |
| HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Microsoft\TestApp |
| HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize |
| HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles |

## READ FILES

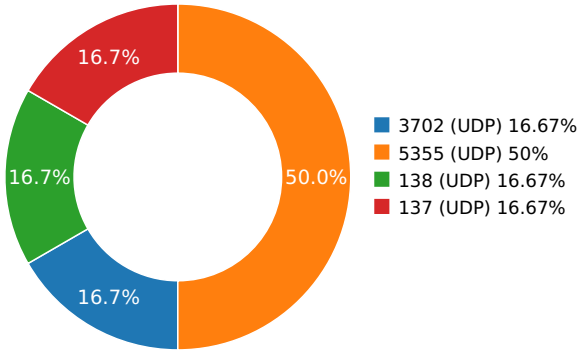
| |
|---|
| \Device\KsecDD |
| C:\Windows\System32\WSHTCPIP.DLL |
| C:\Windows\System32\wship6.dll |
| C:\Windows\System32\wshqos.dll |
| C:\Windows\SysWOW64\en-US\KERNELBASE.dll.mui |
| C:\Windows\System32\tzres.dll |

## 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 |
|---|---|---|---|
| 7.14841794968 | Sandbox | 224.0.0.252 | 5355 |
| 7.22766494751 | Sandbox | 192.168.56.255 | 137 |
| 7.23407888412 | Sandbox | 224.0.0.252 | 5355 |
| 7.23610401154 | Sandbox | 239.255.255.250 | 3702 |
| 9.80351901054 | Sandbox | 224.0.0.252 | 5355 |
| 11.9751060009 | 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:** | 49b7a7484c716ac86421602641bbab7b66a56d52 |
| **File Type:** | PE32 executable (console) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed |
| **SHA1:** | 49b7a7484c716ac86421602641bbab7b66a56d52 |
| **MD5:** | a9602a5006474edb62e4b7a5f38cbf45 |
| **First Seen Date:** | 2019-06-01 07:39:39.214728 ( 3 months ago ) |
| **Number Of Clients Seen:** | 5 |
| **Last Analysis Date:** | 2019-09-06 12:05:10.685295 ( about 17 hours ago ) |
| **Human Expert Analysis Date:** | 2019-06-01 22:20:36.047237 ( 3 months ago ) |
| **Human Expert Analysis Result:** | Malware |

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 | 3 |
| Trid | [] |
| Compilation Time Stamp | 0x0 [Thu Jan 1 00:00:00 1970 UTC] [SUSPICIOUS] |
| Entry Point | 0x893510 (UPX1) |
| Machine Type | Intel 386 or later - 32Bit |
| File Size | 1944576 |
| Ssdeep | |
| Sha256 | eaa361880e9d8e0609cb9e5dce4ad969f6c77737e3c78d9dd714bebc17af0a4d |
| Exifinfo | [] |
| Mime Type | application/x-dosexec |
| Imphash | |

### PE Sections

| NAME | VIRTUAL ADDRESS | VIRTUAL SIZE | RAW SIZE | ENTROPY | MD5 |
|---|---|---|---|---|---|
| UPX0 | 0x1000 | 0x2b8000 | 0x0 | 0.0 | d41d8cd98f00b204e9800998ecf8427e |
| UPX1 | 0x2b9000 | 0x1db000 | 0x1da800 | 7.8757605893 | fb43085eb65dc7460f9618376f247f29 |
| UPX2 | 0x494000 | 0x1000 | 0x200 | 1.76967585909 | 90cacfd3dd45cafe5a84fd9c1e6d0310 |

## CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

## SCREENSHOTS