VALKYRIE COMODO

Summary

File Name: 102687251e7a0f324ed3cca8cf84b9180f24bbdf

File Type: Java archive data (JAR)

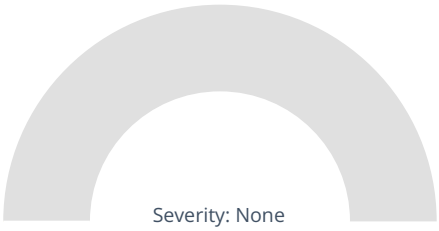
SHA1: 102687251e7a0f324ed3cca8cf84b9180f24bbdf

MD5: e8d864849ff6fa97ce277701eef664a2

CLEAN

Valkyrie Final Verdict

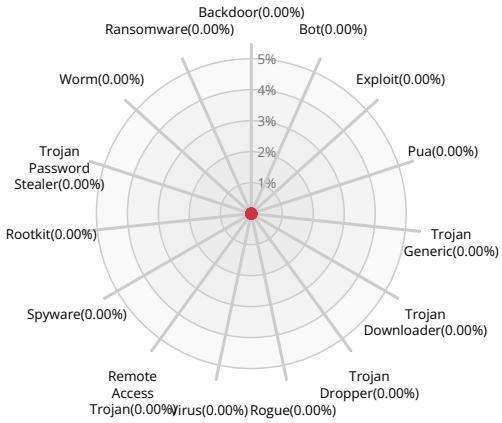
DETECTION SECTION



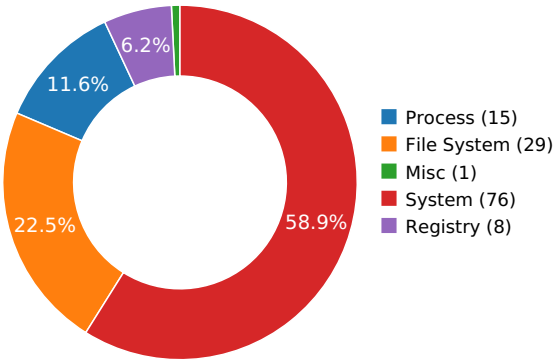
Severity: None

Verdict: Clean

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

MALWARE ANALYSIS SYSTEM EVASION

Network activity detected but not expressed in API logs

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\discord-rpc.dll
C:\Users\user\AppData\Local\Temp\discord-rpc.dll.123.Manifest
C:\Users\user\AppData\Local\Temp\discord-rpc.dll.124.Manifest
C:\Windows\SysWOW64\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\system\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\api-ms-win-core-fibers-l1-1-1.DLL
C:\Users\user\AppData\Local\Temp\api-ms-win-core-fibers-l1-1-1.DLL
C:\ProgramData\Oracle\Java\javapath\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\wbem\api-ms-win-core-fibers-l1-1-1.DLL
C:\Windows\System32\WindowsPowerShell\v1.0\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files\Microsoft Network Monitor 3\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Universal Extractor\bin\api-ms-win-core-fibers-l1-1-1.DLL
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\api-ms-win-core-fibers-l1-1-1.DLL
C:\Python27\Scripts\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\sysinternals\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\api-ms-win-core-fibers-l1-1-1.DLL
C:\tools\IDA_Pro_v6\python\api-ms-win-core-fibers-l1-1-1.DLL

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsSetValue
kernel32.dll.InitializeCriticalSectionEx
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

REGISTRY KEYS

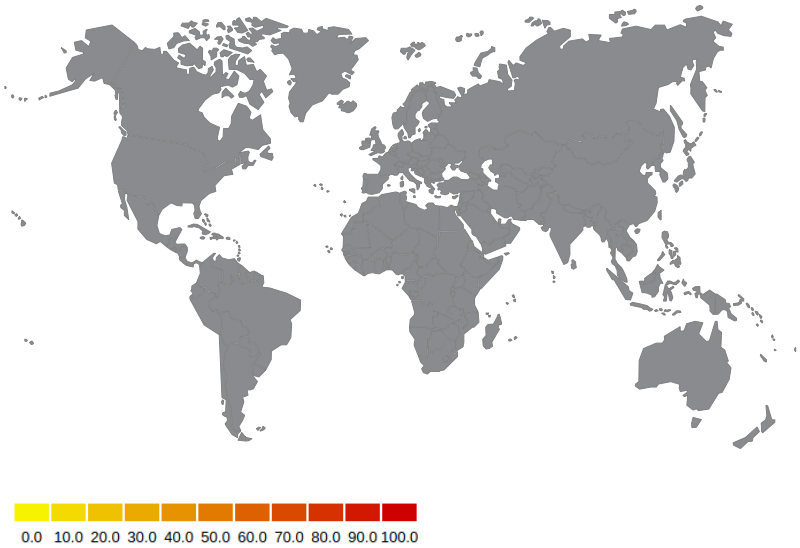
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest

READ FILES

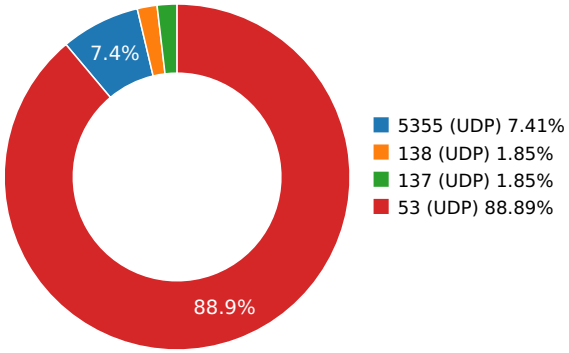
C:\Users\user\AppData\Local\Temp\discord-rpc.dll
C:\Users\user\AppData\Local\Temp\discord-rpc.dll.123.Manifest
C:\Users\user\AppData\Local\Temp\discord-rpc.dll.124.Manifest

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4		15169	Google LLC	Malware Process
	8.8.8.8		15169	Google LLC	Malware Process
					Malware Process
www.aieov.com	45.56.79.23	United States	63949	Akamai Technologies, Inc.	Malware Process

DNS QUERIES

Request	Type
5isohu.com	A
www.aieov.com	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.04729700089	Sandbox	224.0.0.252	5355
3.05529308319	Sandbox	224.0.0.252	5355
3.11960411072	Sandbox	192.168.56.255	137
3.73807096481	Sandbox	224.0.0.252	5355
5.60404706001	Sandbox	224.0.0.252	5355
6.3602669239	Sandbox	8.8.4.4	53
7.35383605957	Sandbox	8.8.8.8	53
9.11937999725	Sandbox	192.168.56.255	138
20.7138900757	Sandbox	8.8.8.8	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
21.7133340836	Sandbox	8.8.4.4	53
35.0727930069	Sandbox	8.8.8.8	53
36.0725290775	Sandbox	8.8.4.4	53
49.6539030075	Sandbox	8.8.8.8	53
50.6509981155	Sandbox	8.8.4.4	53
64.0100331306	Sandbox	8.8.8.8	53
65.0103600025	Sandbox	8.8.4.4	53
78.3696160316	Sandbox	8.8.8.8	53
79.3692760468	Sandbox	8.8.4.4	53
96.6195220947	Sandbox	8.8.8.8	53
97.6195869446	Sandbox	8.8.4.4	53
110.979100943	Sandbox	8.8.8.8	53
111.978825092	Sandbox	8.8.4.4	53
125.338390112	Sandbox	8.8.8.8	53
126.337783098	Sandbox	8.8.4.4	53
143.588454962	Sandbox	8.8.8.8	53
144.587779045	Sandbox	8.8.4.4	53
157.947686911	Sandbox	8.8.8.8	53
158.947251081	Sandbox	8.8.4.4	53
172.308454037	Sandbox	8.8.8.8	53
173.306920052	Sandbox	8.8.4.4	53
190.557976961	Sandbox	8.8.8.8	53
191.561001062	Sandbox	8.8.4.4	53
204.916247129	Sandbox	8.8.8.8	53
205.916474104	Sandbox	8.8.4.4	53
219.275690079	Sandbox	8.8.8.8	53
220.275372028	Sandbox	8.8.4.4	53
237.526535988	Sandbox	8.8.8.8	53
238.526081085	Sandbox	8.8.4.4	53
251.886816025	Sandbox	8.8.8.8	53
252.885106087	Sandbox	8.8.4.4	53
266.24605298	Sandbox	8.8.8.8	53
267.244607925	Sandbox	8.8.4.4	53
284.495224953	Sandbox	8.8.8.8	53
285.494980097	Sandbox	8.8.4.4	53
298.855638981	Sandbox	8.8.8.8	53
299.853701115	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
313.214731932	Sandbox	8.8.8.8	53
314.213757038	Sandbox	8.8.4.4	53
327.466327906	Sandbox	8.8.8.8	53
328.46312809	Sandbox	8.8.4.4	53
341.823595047	Sandbox	8.8.8.8	53
342.822458029	Sandbox	8.8.4.4	53
356.183628082	Sandbox	8.8.8.8	53
357.182217121	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	102687251e7a0f324ed3cca8cf84b9180f24bbdf
File Type:	Java archive data (JAR)
SHA1:	102687251e7a0f324ed3cca8cf84b9180f24bbdf
MD5:	e8d864849ff6fa97ce277701eef664a2
First Seen Date:	2024-02-22 15:09:13.007841 (8 months ago)
Number Of Clients Seen:	5
Last Analysis Date:	2024-07-27 21:38:59.269975 (3 months ago)
Human Expert Analysis Date:	2024-02-24 04:58:51.213991 (8 months ago)
Human Expert Analysis Result:	Clean

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	13
File Type Enum	11
File Size	7171703
Sha256	251940242f44335410ce1878852fdd986d0ee63b5c708c9895ea0f9b198cce86
Mime Type	application/java-archive

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS