VALKYRIE COMODO

Summary

File Name: 555.exe

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

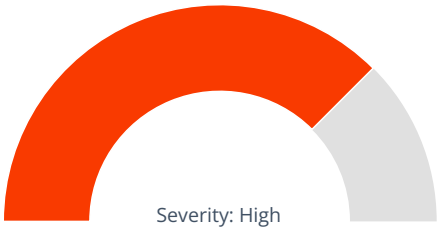
SHA1: e8cbbc2b181c177ffbe414b69a22175b8834b227

MD5: 5efce3ea3ad47d8fecaf22c78579fd4e

MALWARE

Valkyrie Final Verdict

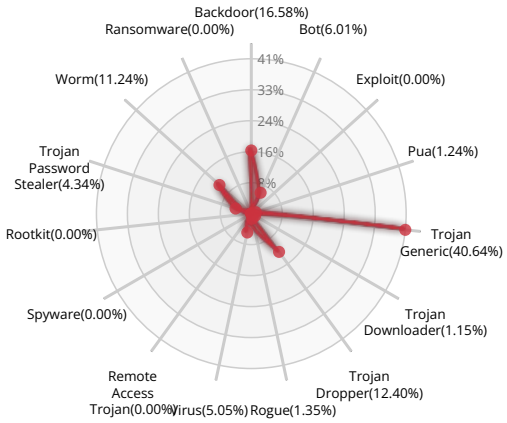
DETECTION SECTION



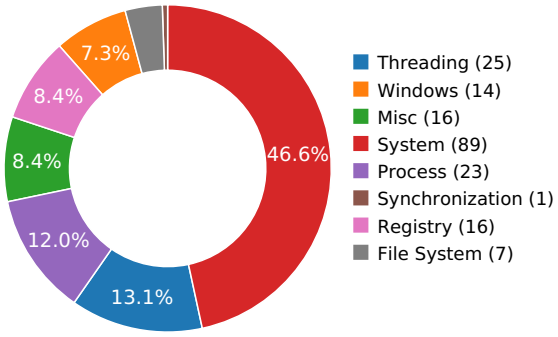
Severity: High

Verdict: Malware

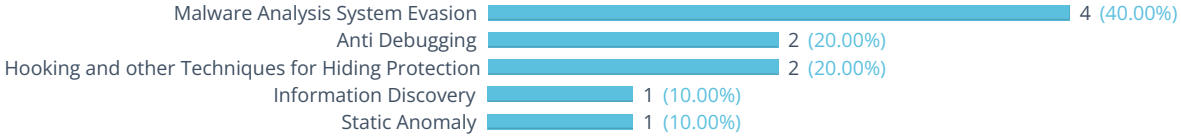
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes	Show sources

STATIC ANOMALY

Anomalous binary characteristics	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Detects VirtualBox through the presence of a registry key	Show sources
Checks the version of Bios, possibly for anti-virtualization	Show sources
Detects the presence of Wine emulator via registry key	Show sources
Network activity detected but not expressed in API logs	

ANTI DEBUGGING

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

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources
The following process appear to have been packed with Themida: e8cbbc2b181c177ffbe414b69a22175b8834b227.exe	

Behavior Graph

Behavior Summary

ACCESSED FILES

\??\SICE
\??\SIWVID
\??\NTICE
C:\Windows\System32\ntdll.dll
C:\Windows\Globalization\Sorting\sortdefault.nls

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\DriverDesc
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\SystemBiosVersion
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\VideoBiosVersion
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

MODIFIED FILES

\??\SICE
\??\SIWVID
\??\NTICE

RESOLVED APIS

kernel32.dll.GetNativeSystemInfo
winmm.dll.timeGetTime
ntdll.dll.NtOpenThread
ntdll.dll.NtQuerySystemInformation
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
ntdll.dll.RtlAllocateHeap

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Wine
HKEY_LOCAL_MACHINE\HARDWARE\ACPI\DSDT\VBOX__
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\CLASS\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000\DriverDesc
HKEY_LOCAL_MACHINE\Hardware\description\System

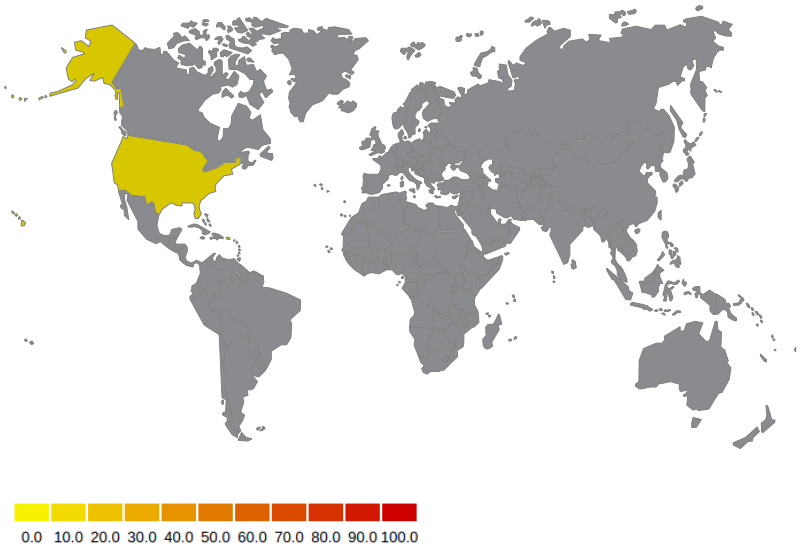
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\SystemBiosVersion
HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\VideoBiosVersion
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

READ FILES

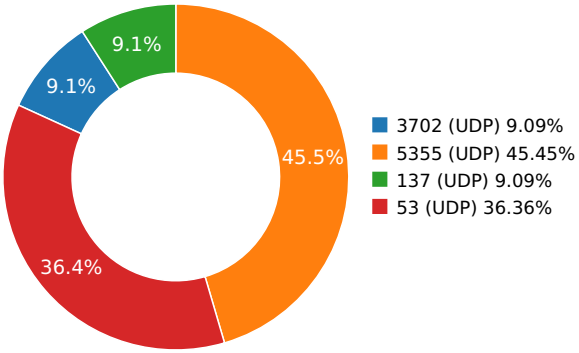
\??\SICE
\??\SIWVID
\??\NTICE
C:\Windows\System32\ntdll.dll
C:\Windows\Globalization\Sorting\sortdefault.nls

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	United States	15169	Google LLC	Malware Process
	23.200.3.7		20940	Akamai Technologies, Inc.	Malware Process
					Malware Process

DNS QUERIES

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

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.24916386604	Sandbox	224.0.0.252	5355
3.25141382217	Sandbox	224.0.0.252	5355
3.25689601898	Sandbox	239.255.255.250	3702
3.31956887245	Sandbox	192.168.56.255	137
4.26933193207	Sandbox	224.0.0.252	5355
5.99251198769	Sandbox	224.0.0.252	5355
6.08753395081	Sandbox	224.0.0.252	5355
7.19613695145	Sandbox	8.8.4.4	53
8.19415998459	Sandbox	8.8.8.8	53
8.72635889053	Sandbox	8.8.4.4	53
9.72626495361	Sandbox	8.8.8.8	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	555.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	e8cbbc2b181c177ffbe414b69a22175b8834b227
MD5:	5efce3ea3ad47d8fecaf22c78579fd4e
First Seen Date:	2024-11-03 12:59:36.391943 (5 months ago)
Number Of Clients Seen:	4
Last Analysis Date:	2024-11-04 18:53:18.431275 (5 months ago)
Human Expert Analysis Date:	2024-12-20 13:54:49.706678 (4 months ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	6
Trid	[]
Compilation Time Stamp	0x67168C77 [Mon Oct 21 17:16:39 2024 UTC]
Entry Point	0x705000 (.taggant)
Machine Type	Intel 386 or later - 32Bit
File Size	2963968
Ssdeep	
Sha256	f1e2bd19183e2d12a66b732f7b78befb199c44182f24a6f903385530b3af230a
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
	0x1000	0x59000	0x28600	7.97900505012	8427b2b686f9ef44b1e0d3435dcafecb
.rsrc	0x5a000	0x340	0x400	4.99738997375	5c7c8122a7854db521db600ca46269e9
.idata	0x5b000	0x1000	0x200	0.999651588151	b36aef970bd1b7d2f5de1064b473cacc
sdftfoxv	0x5c000	0x2a8000	0x2a7600	6.35153597665	63f4b88524d01c035ac1e426ec1ee849
niqosjiw	0x304000	0x1000	0x600	5.05716912684	62d4a64740891f08c1706643a86cfb8b
.taggant	0x305000	0x3000	0x2200	0.769980624655	2dd702d0aab5caa552f79da98ce7ff0b

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_MANIFEST', u'offset': 368728, u'sha256': u'b3a8ff49e0b32b632b3b99a01c3d191f95a8566664da090bfff4652229fe083e', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 742}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS