VALKYRIE COMODO

Summary

File Name: gVQwT.exe

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

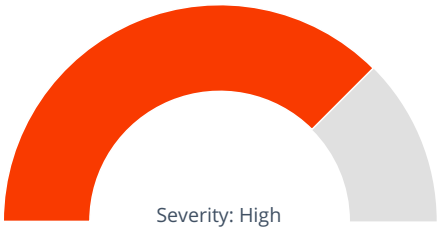
SHA1: bd356d3d2f1e5504a47d5f6d743411c721e4c8f0

MD5: 2c7cb1ce9b000196db3f1ff18c84d879

MALWARE

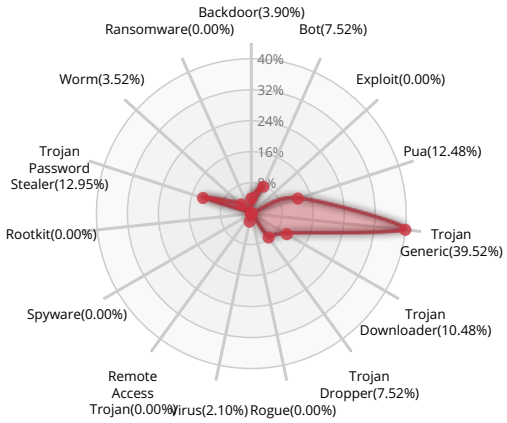
Valkyrie Final Verdict

DETECTION SECTION

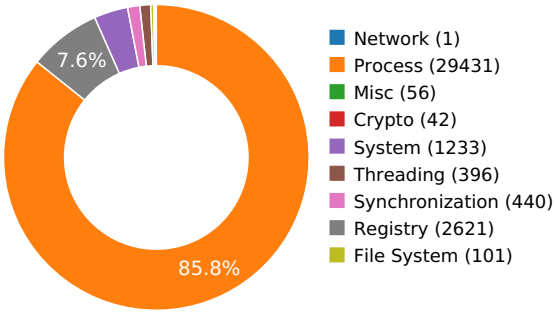


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

INFORMATION DISCOVERY

Reads data out of its own binary image Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

STEALING OF SENSITIVE INFORMATION

Collects information to fingerprint the system Show sources

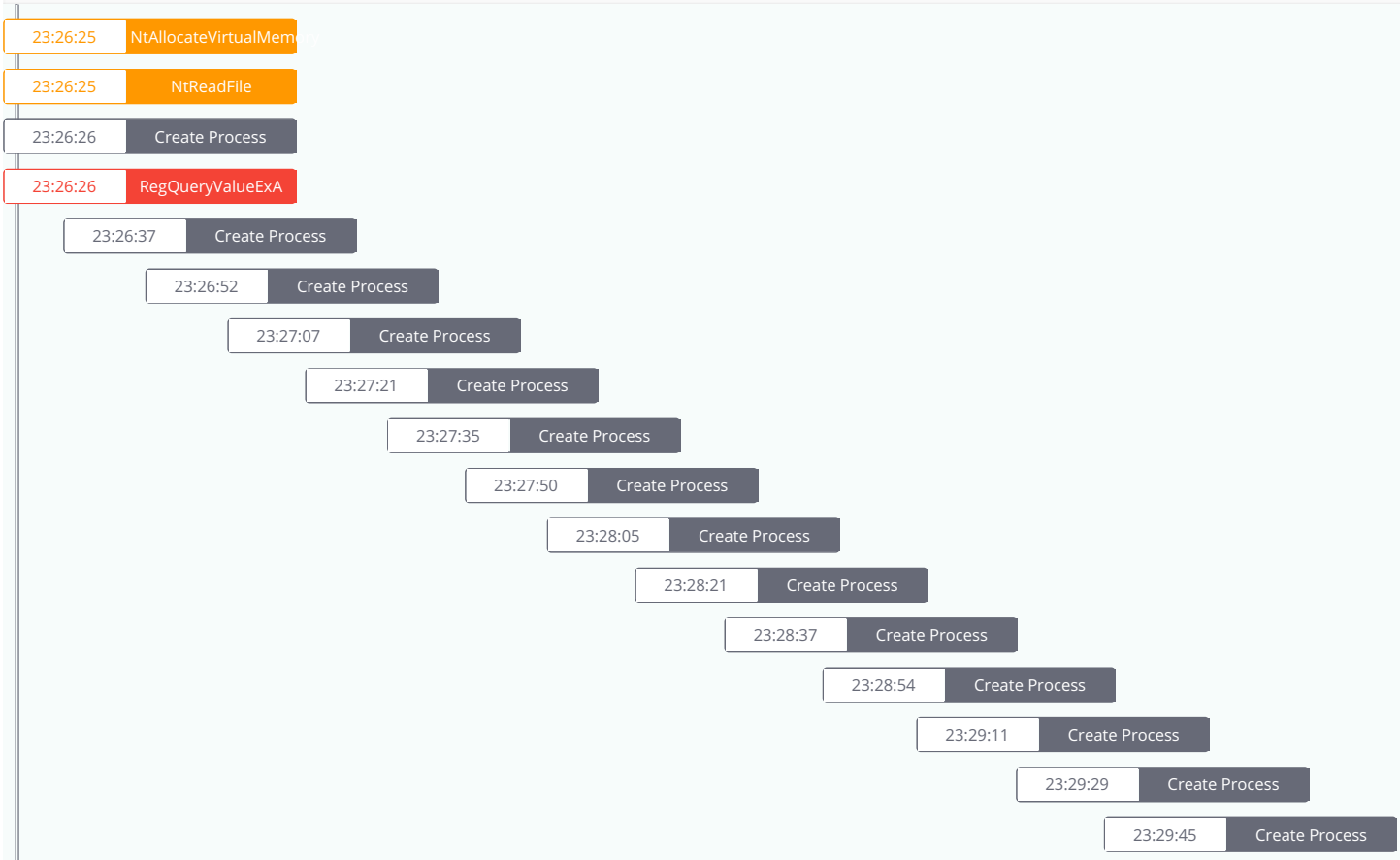
VALKYRIE COMODO

Behavior Graph

23:26:25 **23:28:08** **23:29:51**

PID 2724

23:26:25 **Create Process** The malicious file created a child process as bd356d3d2f1e5504a47d5f6d743411c721e4c8f0.exe **(PPID 2760)**



PID 2464

23:26:26 **Create Process** The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 1840

23:26:39 **Create Process** The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 1136

23:26:57 **Create Process** The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 1888

23:27:19 **Create Process** The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 2880

23:27:37 **Create Process** The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 2976

23:27:53 **Create Process** The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 2840

23:28:06 **Create Process** The malicious file created a child process as svchost.exe **(PPID 2724)**

VALKYRIE COMODO

PID 1576

23:28:18	Create Process	The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 3028

23:28:29	Create Process	The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 2448

23:28:40	Create Process	The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 2208

23:28:54	Create Process	The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 1540

23:29:10	Create Process	The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 2252

23:29:30	Create Process	The malicious file created a child process as svchost.exe **(PPID 2724)**

PID 2740

23:29:51	Create Process	The malicious file created a child process as svchost.exe **(PPID 2724)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\SysWOW64*.dll
C:\Users*
C:\Windows\System32*.exe
C:\Users\user\AppData\Local\Temp\bd356d3d2f1e5504a47d5f6d743411c721e4c8f0.exe

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_CURRENT_USER\Volatile Environment\USERNAME
HKEY_CURRENT_USER\Volatile Environment\USERDOMAIN
HKEY_CURRENT_USER\Volatile Environment\APPDATA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension

RESOLVED APIS

kernel32.dll.VirtualAlloc
kernel32.dll.LoadLibraryA
kernel32.dll.GetProcAddress
kernel32.dll.VirtualProtect
kernel32.dll.FreeConsole
kernel32.dll.VirtualQuery
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
cryptsp.dll.CryptAcquireContextW

cryptsp.dll.CryptCreateHash
cryptsp.dll.CryptHashData
cryptsp.dll.CryptGetHashParam
cryptsp.dll.CryptDestroyHash
cryptsp.dll.CryptReleaseContext
ntmarta.dll.GetMartaExtensionInterface
kernel32.dll.ExitThread
kernel32.dll.HeapAlloc
kernel32.dll.HeapReAlloc

REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\crypt32
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\crypt32\DebugHeapFlags
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\DisableImprovedZoneCheck
HKEY_LOCAL_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\Internet Settings
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\Internet Settings\Security_HKLM_only
HKEY_USERS\
HKEY_USERS\.DEFAULT
HKEY_USERS\.DEFAULT\
HKEY_USERS\S-1-5-19
HKEY_USERS\S-1-5-19\
HKEY_USERS\S-1-5-20
HKEY_USERS\S-1-5-20\
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000
HKEY_CURRENT_USER\
HKEY_CURRENT_USER\Volatile Environment
HKEY_CURRENT_USER\Volatile Environment\USERNAME
HKEY_CURRENT_USER\Volatile Environment\USERDOMAIN
HKEY_CURRENT_USER\Volatile Environment\APPDATA
HKEY_LOCAL_MACHINE\
HKEY_LOCAL_MACHINE\SOFTWARE
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion

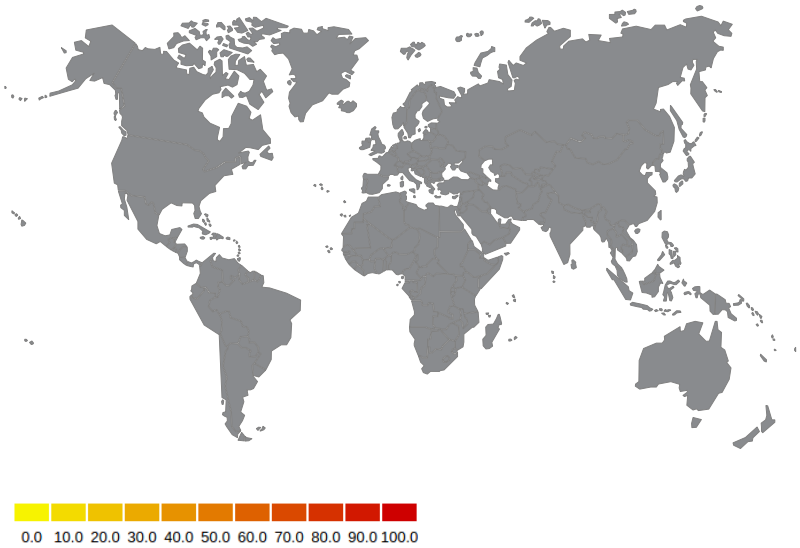
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\InstallDate
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA\AccessProviders
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Lsa\AccessProviders\MartaExtension

MUTEXES

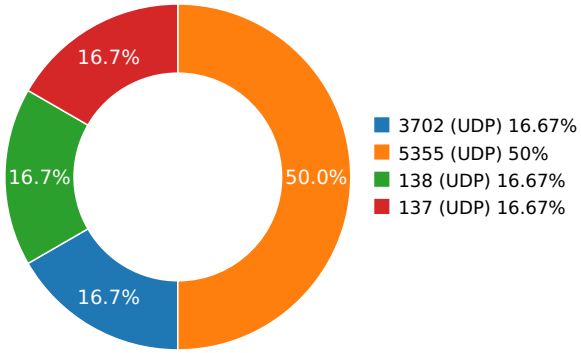
{85d3790e-baa9-6105-70b4-1a7e92572918}
{14cba3df-b7ed-9d8c-240c-24e533fdfc64}
{6336aa74-ae16-e6c8-8cd6-feeacd6e3bd0}
{c7281f10-2f87-a74c-2a20-2d64ece47557}
{c8f702a8-cbfb-e181-9e75-d06d91540b0a}
{fbdf3e68-fffd-fe18-477c-a94c1bbf705d}
{ddfa361b-ea7b-00c6-de38-67241850096b}
{636158df-7139-1d1f-658b-9b41034a6af3}
{db38a22b-52ca-7410-1c00-e9039216e7a1}
{613dc117-1a7a-c0b3-61ca-5b830604d170}
{11e9708b-503e-6213-185e-04ef3b2ab393}
{84867105-b595-de4b-b228-235b2e8da285}
{c814c39d-f005-bacf-4316-f7e57ac2e31d}
{b355d625-3105-6422-c633-2450c2d13662}

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
7.26307296753	Sandbox	224.0.0.252	5355
7.28605389595	Sandbox	224.0.0.252	5355
7.29079604149	Sandbox	239.255.255.250	3702
7.33592510223	Sandbox	192.168.56.255	137
9.83942604065	Sandbox	224.0.0.252	5355
13.3347790241	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:	gVQwT.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
SHA1:	bd356d3d2f1e5504a47d5f6d743411c721e4c8f0
MD5:	2c7cb1ce9b000196db3f1ff18c84d879
First Seen Date:	2018-03-14 18:44:46.238389 (12 months ago)
Number Of Clients Seen:	3
Last Analysis Date:	2018-03-14 18:44:46.238389 (12 months ago)
Human Expert Analysis Date:	2018-03-14 20:05:07.597076 (12 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	5
Trid	[]
Compilation Time Stamp	0x0 [Thu Jan 1 00:00:00 1970 UTC] [SUSPICIOUS]
Entry Point	0x401bc0 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	143360
Ssdeep	
Sha256	1f79b551e1a35964691ebe1d424b23b571408098c14cc6ae26429962e91d89f7
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xe2a	0x1000	5.96458508508	bbffbda161b8086e6f930913cff97ff1
CODE	0x2000	0x24d6	0x3000	5.0546338917	1f45ae989a55aa0c87aa796707649dd1
.rdata	0x5000	0x770	0x1000	2.52947135342	cef67e0796c0c695575937872840439d
.data	0x6000	0x1cc98	0x1c000	7.16522022568	15240aeca754fb6d8423595f98d39e7d
.reloc	0x23000	0x682	0x1000	0.605596058441	c69bccc99071e861929aa1d25f8aac75

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

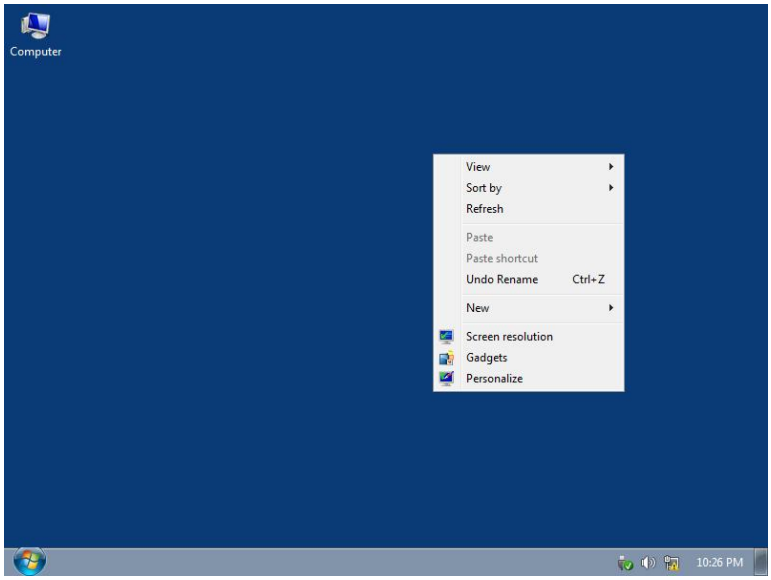
SCREENSHOTS

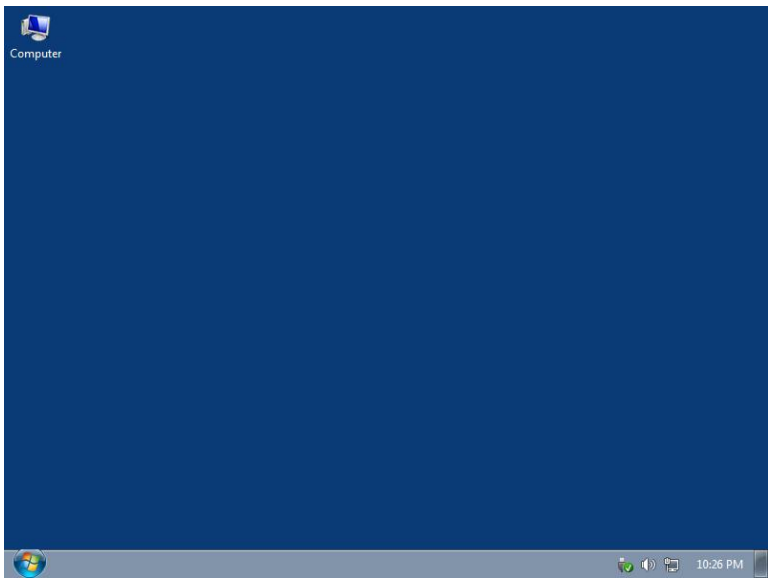

Computer
10:29 PM


Computer
10:26 PM


Computer
10:28 PM


Computer
10:28 PM


Computer
View
Sort by
Refresh
Paste
Paste shortcut
Undo Rename Ctrl+Z
New
Screen resolution
Gadgets
Personalize
10:26 PM


Computer
10:26 PM


Computer
10:29 PM


Computer
Network 4
No Internet access
10:28 PM


Computer
10:28 PM