Summary

File Name: eabe29e9075caa5d067d979cf32082336ef1ba58a2094a2d1f2842bc94d6dcfb

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

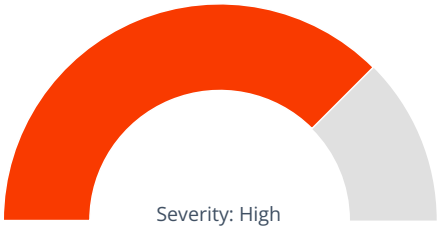
SHA1: 1c8fa769548b32928a92c0a5adb487fb045f21e1

MD5: b794c632c97cdf436161096ef41323c7

MALWARE

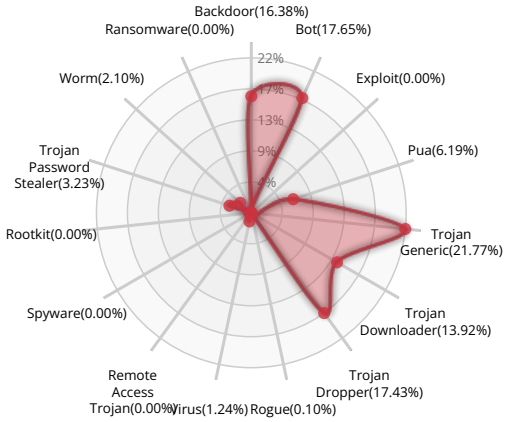
Xcitium Verdict Cloud Final Verdict

DETECTION SECTION

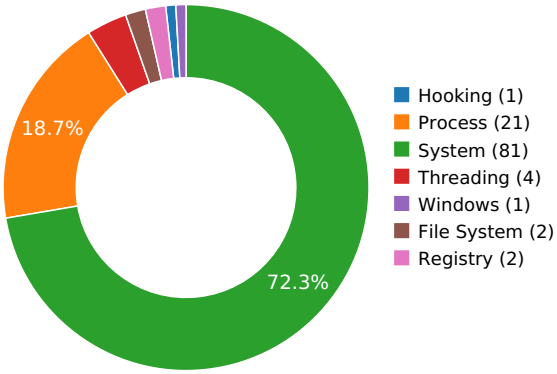


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Activity Details

MALWARE ANALYSIS SYSTEM EVASION

Detects Sandboxie through the presence of a library — Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory — Show sources

Executed a process and injected code into it, probably while unpacking — Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Detects Avast Antivirus through the presence of a library — Show sources

Behavior Graph

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\apfHQ
C:\Windows\System32\ntdll.dll

RESOLVED APIS

kernel32.dll.FlsAlloc
kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.IsProcessorFeaturePresent
kernel32.dll.GlobalAlloc
kernel32.dll.GetLastError
kernel32.dll.Sleep
kernel32.dll.VirtualAlloc
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.Module32First
kernel32.dll.CloseHandle
user32.dll.MessageBoxA
user32.dll.GetMessageExtraInfo
kernel32.dll.WinExec
kernel32.dll.CreateFileA
kernel32.dll.WriteFile
kernel32.dll.CreateProcessA
kernel32.dll.GetThreadContext
kernel32.dll.VirtualAllocEx
kernel32.dll.VirtualFree
kernel32.dll.ReadProcessMemory
kernel32.dll.WriteProcessMemory
kernel32.dll.SetThreadContext
kernel32.dll.ResumeThread
kernel32.dll.WaitForSingleObject
kernel32.dll.GetModuleFileNameA
kernel32.dll.GetCommandLineA
ntdll.dll.NtUnmapViewOfSection

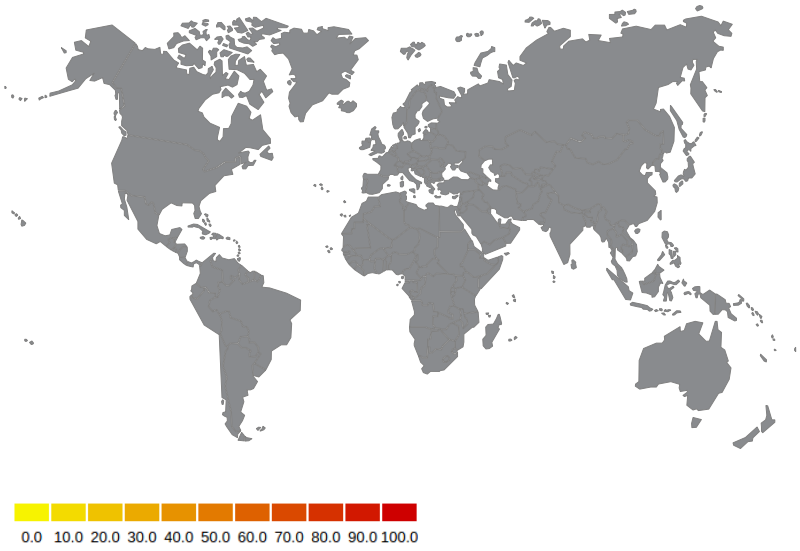
ntdll.dll.NtWriteVirtualMemory
user32.dll.RegisterClassExA
user32.dll.CreateWindowExA
user32.dll.PostMessageA
user32.dll.GetMessageA
user32.dll.DefWindowProcA
kernel32.dll.GetFileAttributesA
kernel32.dll.GetStartupInfoA
kernel32.dll.VirtualProtectEx
kernel32.dll.ExitProcess
uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
dwmapi.dll.DwmIsCompositionEnabled

REGISTRY KEYS

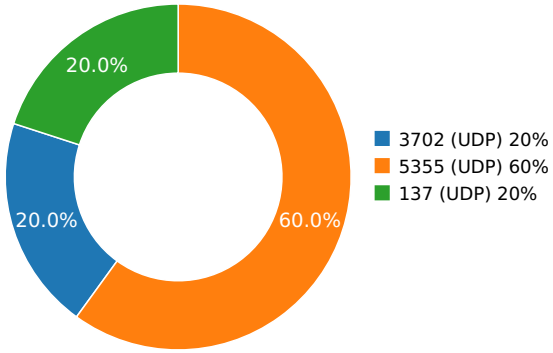
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles

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
3.03705787659	Sandbox	224.0.0.252	5355
3.03799796104	Sandbox	224.0.0.252	5355
3.03902482986	Sandbox	239.255.255.250	3702
3.07942485809	Sandbox	192.168.56.255	137
5.62618088722	Sandbox	224.0.0.252	5355

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	eabe29e9075caa5d067d979cf32082336ef1ba58a2094a2d1f2842bc94d6dcfb
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	1c8fa769548b32928a92c0a5adb487fb045f21e1
MD5:	b794c632c97cdf436161096ef41323c7
First Seen Date:	2022-01-23 20:11:57.525406 (2 years ago)
Number Of Clients Seen:	2
Last Analysis Date:	2022-01-23 20:11:57.525406 (2 years ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[{u'Path': u'C:\\turivi66\\geh seheyoniveveke9_cocinebikove nali_lisuw jiwag\\v.pdb\x00', u'GUID': u'{7ca9eff6-859e-49b0-841f-16d49a4f5ce2}', u'timestamp': u'2022-01-16 11:54:48'}]
Number Of Sections	4
Trid	[[41.0, u'Win32 Executable MS Visual C++ (generic)'], [36.3, u'Win64 Executable (generic)'], [8.6, u'Win32 Dynamic Link Library (generic)'], [5.9, u'Win32 Executable (generic)'], [2.6, u'OS/2 Executable (generic)']]
Compilation Time Stamp	0x5F25A00A [Sat Aug 1 17:02:02 2020 UTC]
ProjectVersion	1.10.74.57
InternationalName	bomgveoci.iwa
FileVersion	21.29.11.69
Copyright	Copyrighz (C) 2021, fudkorta
Translations	0x0121 0x03ca
Entry Point	0x40233e (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	254976
Ssdeep	3072:AJrOL33JjPit56HkU3zjbVx11BFM/h3Lfed:AJqL33ZRbVx1/FN
Sha256	eabe29e9075caa5d067d979cf32082336ef1ba58a2094a2d1f2842bc94d6dcfb
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/c/8/f/1c8fa769548b32928a92c0a5adb487fb045f21e1', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2022:01:23 20:11:47+00:00', u'EXE:InitializedDataSize': 220672, u'File:FileModifyDate': u'2022:01:23 20:10:52+00:00', u'EXE:FileVersionNumber': u'12.0.0.0', u'File:FileSize': u'249 kB', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Unknown (0x60474)', u'EXE:ObjectFileType': u'Static library', u'File:FileType': u'Win32 EXE', u'EXE:UninitializedDataSize': 0, u'File:FileName': u'1c8fa769548b32928a92c0a5adb487fb045f21e1', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 5.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2020:08:01 17:02:02+00:00', u'EXE:FileFlagsMask': u'0x058c', u'EXE:LinkerVersion': 9.0, u'EXE:FileFlags': u'Private build, Info inferred, Special build', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/1/c/8/f', u'EXE:EntryPoint': u'0x233e', u'EXE:SubsystemVersion': 5.0, u'EXE:CodeSize': 57344, u'File:FileInodeChangeDate': u'2022:01:23 20:11:42+00:00', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'23.0.0.0'}]
Mime Type	application/x-dosexec
Imphash	053499f9f514a07786ff9cf8115e6a28

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xde30	0xe000	6.67848093067	ee34b22b60e6c80c5095bac4a7334b7f
.rdata	0xf000	0x3834	0x3a00	3.97020780488	8a84fab9a9badd5f17ce94a48cac42b0
.data	0x13000	0x21d88	0x1d400	3.1517891867	97b45e726fea705afca7cf9aa6c9bd5e
.rsrc	0x35000	0xf1a0	0xf200	6.65149850847	49c4c6ac872b45a0cd9f3fe907cc0d60

PE Imports

- KERNEL32.dll
  - GetDateFormatW
  - GetNativeSystemInfo
  - lstrcpynA
  - FindActCtxSectionGuid
  - InterlockedDecrement
  - SetMailslotInfo
  - GetProfileSectionA
  - GetComputerNameW
  - SetEvent
  - GetConsoleAliasesLengthA
  - SetFileTime
  - GlobalAlloc
  - SwitchToFiber
  - Sleep
  - DeleteVolumeMountPointW
  - GetStringTypeExW
  - DnsHostnameToComputerNameW
  - RaiseException
  - LCMapStringA
  - GetProcAddress
  - VirtualAlloc
  - PeekConsoleInputW
  - RemoveDirectoryA
  - SetStdHandle
  - SetFileAttributesA
  - GetAtomNameA
  - LocalAlloc
  - GetModuleFileNameA
  - GetModuleHandleA
  - SetLocaleInfoW
  - GetConsoleTitleW
  - GetCurrentThreadId
  - ReadConsoleInputW
  - GetConsoleProcessList
  - lstrcpyW
  - UnhandledExceptionFilter
  - SetUnhandledExceptionFilter
  - GetStartupInfoW
  - HeapAlloc
  - TerminateProcess
  - GetCurrentProcess
  - IsDebuggerPresent
  - EnterCriticalSection
  - LeaveCriticalSection
  - GetModuleHandleW
  - ExitProcess
  - GetLastError
  - WriteFile
  - GetStdHandle
  - SetHandleCount
  - GetFileType
  - GetStartupInfoA
  - DeleteCriticalSection
  - SetFilePointer
  - HeapFree
  - CloseHandle
  - GetModuleFileNameW
  - FreeEnvironmentStringsW
  - GetEnvironmentStringsW
  - GetCommandLineW

    - TlsGetValue
    - TlsAlloc
    - TlsSetValue
    - TlsFree
    - InterlockedIncrement
    - SetLastError
    - HeapCreate
    - VirtualFree
    - QueryPerformanceCounter
    - GetTickCount
    - GetCurrentProcessId
    - GetSystemTimeAsFileTime
    - HeapReAlloc
    - ReadFile
    - GetCPInfo
    - GetACP
    - GetOEMCP
    - IsValidCodePage
    - WideCharToMultiByte
    - RtlUnwind
    - LoadLibraryA
    - InitializeCriticalSectionAndSpinCount
    - GetConsoleCP
    - GetConsoleMode
    - FlushFileBuffers
    - MultiByteToWideChar
    - LCMapStringW
    - GetStringTypeA
    - GetStringTypeW
    - GetLocaleInfoA
    - HeapSize
    - WriteConsoleA
    - GetConsoleOutputCP
    - WriteConsoleW
    - CreateFileA
- WINHTTP.dll
    - WinHttpOpen

PE Resources

{u'lang': u'LANG_GREEK', u'name': u'KUNADOREHUMENANAMOVIZO', u'offset': 267584, u'sha256': u'2856182b736f59c8f69da37669b78769a4613822d7d21748cb9fbd0c7bf8dc00', u'type': u'ASCII text, with very long lines, with no line terminators', u'size': 9441}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 218432, u'sha256': u'34b07a038cc6fa2f46ff1329ff4befd4a9c17651b72fb046fbe34eab84161fc8', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 222184, u'sha256': u'cfa5d2805e1343a6373a65b74b67a6649144f4d2c03673ed5a402b22ec5c9c86', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 224400, u'sha256': u'95527a47a9f298029454e1e9b14aea3cea4dcdac491975c7cc56748735e107c5', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 225784, u'sha256': u'81c84884758b4920032747dcefd80435d0cc4194b747b288034a9ccab810eabd', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 235424, u'sha256': u'407cd88c4cb5098ebc72c00734ee0bd96e2c1943201da12b074275e071479003', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 239688, u'sha256': u'36ade83131d80772ad30795736cc5e5a67eb2cad7bbae3b0da86c588ff074b7d', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 242128, u'sha256': u'6574073f2a6d5c251fb9cbc2667f6c88180d92657e76b0bfc4b895dd6c84e026', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 243360, u'sha256': u'26bb9bf4ad4c6ce7ccf39fa8ff901e0ed4b00aae88c3ab19526bf4f3bfea96f2', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 247112, u'sha256': u'ce6fd7a4281d97e0144fbfd6bae3282e71b27fa3069903281f14fb0f0f9a1125', u'type': u'data', u'size': 2216}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 249328, u'sha256': u'6376c8a2ed20c7fb90d68e99bc6e78516119bfeb87426e7b4f53ff4119536d36', u'type': u'data', u'size': 1736}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 251064, u'sha256': u'08ac6dc367ae6e817d00b911dd51764460ff1e482dd97f9cef8ae6b6a794611c', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1384}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 252448, u'sha256': u'43da28b40b2b690a59f8b5f0b7de9acd82b13d38b1e4a70939b90b1abdc7706d', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 262088, u'sha256': u'b70158eaaf20c3bb0f4d64a1c7e265a0eadb040bca77a2ad23d1591ae367cdb2', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_GREEK', u'name': u'RT_ICON', u'offset': 266352, u'sha256': u'e83211b7fc5fae4e6a53a4907a5d76b6025c4a161ac531a81fa058256261c340', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_GREEK', u'name': u'RT_STRING', u'offset': 277680, u'sha256': u'1351c6d7f1ccd139d30ba0e2e9083eaecf34e3b3e4bb201d26e3ba4cbf4c6b63', u'type': u'data', u'size': 554}

{u'lang': u'LANG_GREEK', u'name': u'RT_STRING', u'offset': 278240, u'sha256': u'358139544a5e073c3fca007edad0a2a2d637e747682155cce4bbe74566ad2624', u'type': u'data', u'size': 704}

{u'lang': u'LANG_GREEK', u'name': u'RT_ACCELERATOR', u'offset': 277032, u'sha256': u'c49f2d4cb53185d33d07cb323ad4874925c9753bba50335cc26edf22a724e1d2', u'type': u'data', u'size': 96}

{u'lang': u'LANG_GREEK', u'name': u'RT_ACCELERATOR', u'offset': 277128, u'sha256': u'e2159beadc29f552eba7dcbedb153c25e7b22b6ac5e2a26983a6084073f28393', u'type': u'data', u'size': 32}

{u'lang': u'LANG_GREEK', u'name': u'RT_GROUP_ICON', u'offset': 243256, u'sha256': u'582b16b3a55169ebdd7885cfa96227e80a971f13f6b395fe0469e06e2ce8b800', u'type': u'MS Windows icon resource - 7 icons, 48x48', u'size': 104}

{u'lang': u'LANG_GREEK', u'name': u'RT_GROUP_ICON', u'offset': 267480, u'sha256': u'ca298653902d652a2541c49f4faea798104b80165022f0a3e0a4b60ee737469e', u'type': u'MS Windows icon resource - 7 icons, 48x48', u'size': 104}

{u'lang': u'LANG_GREEK', u'name': u'RT_VERSION', u'offset': 277176, u'sha256': u'64d48b7963921f69038faec4ab457f52d806a55970af0136d02d53280da05bcd', u'type': u'data', u'size': 500}

{u'lang': u'LANG_GREEK', u'name': u'241', u'offset': 277160, u'sha256': u'3a0e57bb42b1b053de642b15c60007f7ac0e1ffc079ff2e9374489ec9bd21789', u'type': u'data', u'size': 10}

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS