VALKYRIE COMODO

Summary

File Name: 1705011010.exe

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

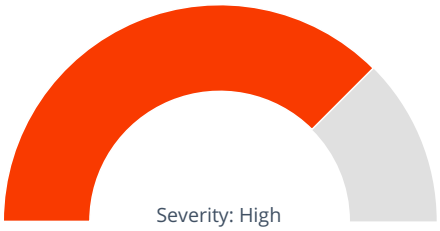
SHA1: 9f104ffe6f6817235d1da0947b601c5f9bf014af

MD5: b71d80ba5c8467471def36580a98bcfd

MALWARE

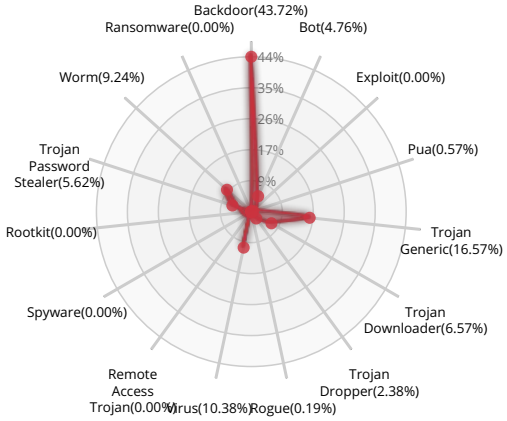
Valkyrie Final Verdict

DETECTION SECTION

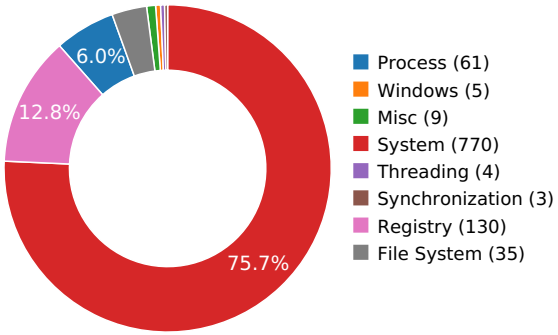


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Reads data out of its own binary image Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory

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

Behavior Graph

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\9f104ffe6f6817235d1da0947b601c5f9bf014af.exe
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\9f104ffe6f6817235d1da0947b601c5f9bf014af.ex_
C:\Users\user\AppData\Local\CSIDL_X
C:\Users\user\AppData\Local\CSIDL_
C:\myapp.exe
C:\Windows\explorer.exe\

READ REGISTRY KEYS

HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List\File1
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List\File2
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List\File3
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List\File4
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Settings\PreviewPages
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16

MODIFIED FILES

C:\Users\user\AppData\Local\Temp\9f104ffe6f6817235d1da0947b601c5f9bf014af.ex_

C:\Users\user\AppData\Local\Temp\9f104ffe6f6817235d1da0947b601c5f9bf014af.exe

RESOLVED APIS

dwmapi.dll.DwmIsCompositionEnabled

gdi32.dll.GetLayout

gdi32.dll.GdiRealizationInfo

gdi32.dll.FontIsLinked

advapi32.dll.RegOpenKeyExW

advapi32.dll.RegQueryInfoKeyW

gdi32.dll.GetTextFaceAliasW

advapi32.dll.RegEnumValueW

advapi32.dll.RegCloseKey

advapi32.dll.RegQueryValueExW

gdi32.dll.GetFontAssocStatus

advapi32.dll.RegQueryValueExA

advapi32.dll.RegEnumKeyExW

gdi32.dll.GetTextExtentExPointWPri

comctl32.dll.InitCommonControlsEx

comctl32.dll.DllGetVersion

user32.dll.NotifyWinEvent

kernel32.dll.GetModuleFileNameW

kernel32.dll.CreateFileW

kernel32.dll.VirtualAlloc

kernel32.dll.GetFileSize

kernel32.dll.ReadFile

kernel32.dll.CloseHandle

shell32.dll.SHGetSpecialFolderPathW

kernel32.dll.CopyFileW

kernel32.dll.SetFileAttributesW

kernel32.dll.GetProcAddress

kernel32.dll.GetModuleHandleA
kernel32.dll.GetModuleFileNameA
kernel32.dll.CreateProcessA
kernel32.dll.CreateProcessW
kernel32.dll.OpenMutexA
kernel32.dll.CreateMutexA
kernel32.dll.CreateFileA
kernel32.dll.GetSystemDirectoryA
kernel32.dll.GetSystemDirectoryW
kernel32.dll.MoveFileExW
shell32.dll.SHGetSpecialFolderPathA
advapi32.dll.RegOpenKeyExA
advapi32.dll.RegSetValueExA
advapi32.dll.RegSetValueExW
kernel32.dll.CreateDirectoryW
kernel32.dll.Sleep
kernel32.dll.GetFileTime
kernel32.dll.SetFileTime
kernel32.dll.DeleteFileW
kernel32.dll.ExitProcess
kernel32.dll.GetTickCount
kernel32.dll.GetCurrentProcess
kernel32.dll.GlobalAlloc
advapi32.dll.OpenProcessToken
advapi32.dll.GetTokenInformation
advapi32.dll.AllocateAndInitializeSid
advapi32.dll.EqualSid
advapi32.dll.LookupAccountSidA
kernel32.dll.CreateToolhelp32Snapshot
kernel32.dll.Process32First
kernel32.dll.Process32Next
kernel32.dll.Module32First
kernel32.dll.Module32Next
ntdll.dll.NtUnmapViewOfSection
kernel32.dll.VirtualAllocEx

kernel32.dll.WriteProcessMemory
kernel32.dll.GetThreadContext
kernel32.dll.SetThreadContext
kernel32.dll.ResumeThread
kernel32.dll.SuspendThread
kernel32.dll.TerminateProcess
ntdll.dll.NtReadVirtualMemory
kernel32.dll.IsWow64Process
kernel32.dll.OpenProcess
kernel32.dll.DuplicateHandle
psapi.dll.GetProcessMemoryInfo
kernel32.dll.GetCommandLineW
kernel32.dll.WriteFile
kernel32.dll.FlsGetValue

REGISTRY KEYS

HKEY_CURRENT_USER\software
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List\File1
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List\File2
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List\File3
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List\File4
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Settings
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Settings\PreviewPages
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\System\CurrentControlSet\Control\Nls\Locale
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale\Alternate Sorts
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontLink\SystemLink
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0\DataFilePath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane1
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane3
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane5
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane6
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane8
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane10
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane11
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane12
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane13
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane14
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane15
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Plane16
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Segoe UI
HKEY_CURRENT_USER

READ FILES

C:\Users\user\AppData\Local\Temp\9f104ffe6f6817235d1da0947b601c5f9bf014af.exe
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\CSIDL_X
C:\Users\user\AppData\Local\Temp\9f104ffe6f6817235d1da0947b601c5f9bf014af.ex_
C:\Users\user\AppData\Local\CSIDL_
C:\myapp.exe

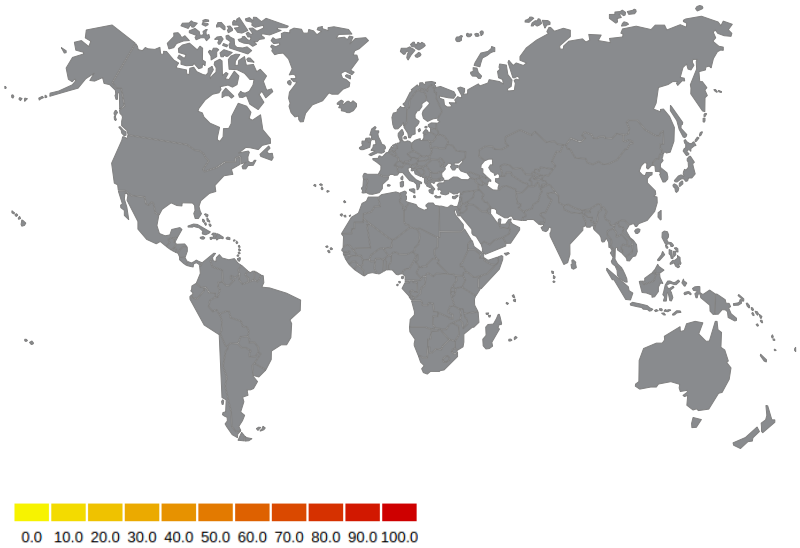
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Recent File List

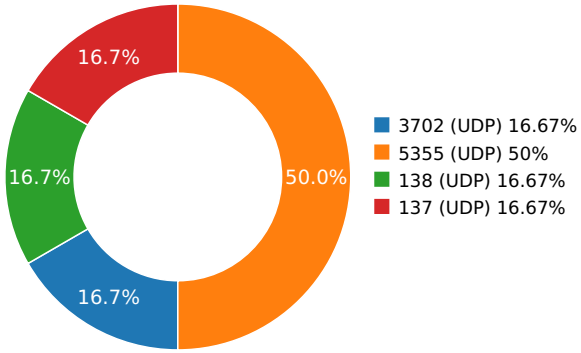
HKEY_CURRENT_USER\Software\Local AppWizard-Generated Applications\CustomPrint\Settings

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
3.11778593063	Sandbox	224.0.0.252	5355
3.13424897194	Sandbox	224.0.0.252	5355
3.1408188343	Sandbox	239.255.255.250	3702
3.18095493317	Sandbox	192.168.56.255	137
5.70085287094	Sandbox	224.0.0.252	5355
9.18054080009	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:	1705011010.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	9f104ffe6f6817235d1da0947b601c5f9bf014af
MD5:	b71d80ba5c8467471def36580a98bcfd
First Seen Date:	2017-05-01 16:16:12.342030 (2 years ago)
Number Of Clients Seen:	8
Last Analysis Date:	2017-05-01 16:16:12.342030 (2 years ago)
Human Expert Analysis Date:	2017-05-02 01:29:19.093104 (2 years ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Number Of Sections	6
Compilation Time Stamp	0x58FA3088 [Fri Apr 21 16:17:12 2017 UTC]
Entry Point	0x2013806 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	366434
Sha256	be7678a2c62ee93e52b73287873cdd8791580076eaa286f5afe8a124b285211a
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x14c73	0x15000	4.153114	-
.rdata	0x16000	0xd3e	0x1000	3.102434	-
.data	0x17000	0x914	0x1000	0.327826[SUSPICIOUS]	-
.idata	0x18000	0xc99	0x1000	3.459574	-
.rsrc	0x19000	0x6344	0x7000	5.812523	-
.reloc	0x20000	0x7ad	0x1000	2.956748	-

PE Imports

- MFC42
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None

    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None

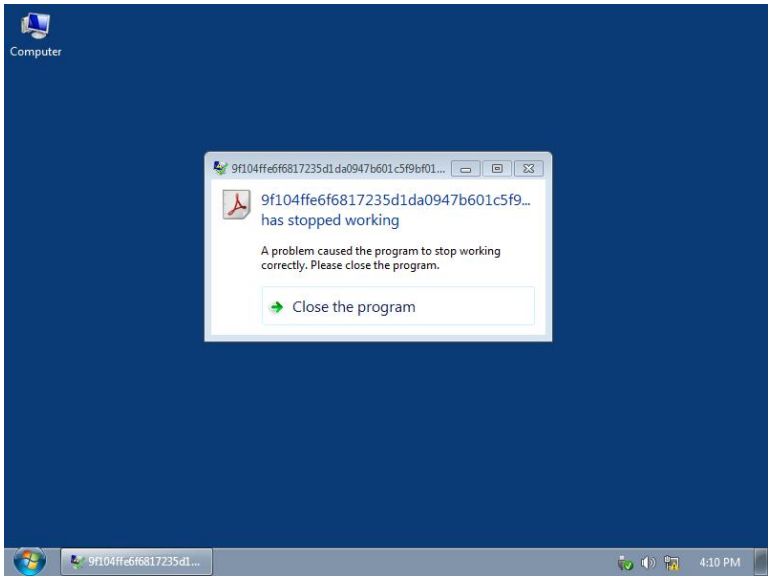
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None
- None

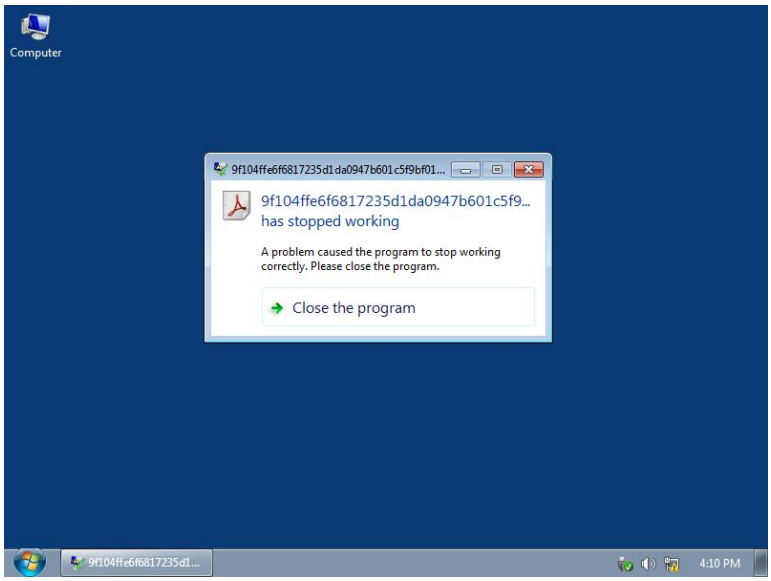
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
    - None
- MSVCRT.dll
    - _acmdln
    - __getmainargs
    - _initterm
    - __setusermatherr
    - _adjust_fdiv
    - __p__commode
    - __p__fmode
    - __set_app_type
    - _except_handler3
    - _controlfp
    - _exit
    - _onexit
    - __dllonexit
    - _ftol
    - __CxxFrameHandler
    - exit
    - _setmbcp
    - _XcptFilter
- KERNEL32.dll
    - CreateFileW
    - GetModuleHandleA
    - GetStartupInfoA
    - GetModuleFileNameW
- USER32.dll
    - UpdateWindow
    - FindWindowW
    - SendMessageA
    - EnableWindow

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS


Computer
9f104ffe6f6817235d1da0947b601c5f9bf01...
9f104ffe6f6817235d1da0947b601c5f9...
has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
9f104ffe6f6817235d1...
4:10 PM


Computer
9f104ffe6f6817235d1da0947b601c5f9bf01...
9f104ffe6f6817235d1da0947b601c5f9...
has stopped working
A problem caused the program to stop working correctly. Please close the program.
Close the program
9f104ffe6f6817235d1...
4:10 PM


Computer
4:10 PM


Computer
4:10 PM