VALKYRIE COMODO

Summary

File Name: decrypter.exe

File Type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed

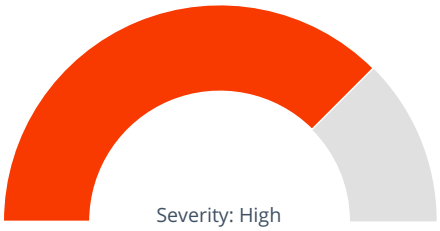
SHA1: c0e993fa53b4d63bf2775c9bf42027fc1257f88c

MD5: 8932a7c2d3d33c5fe46252f3c8713696

MALWARE

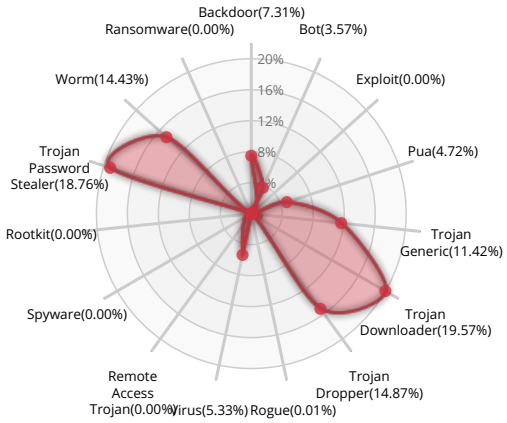
Valkyrie Final Verdict

DETECTION SECTION

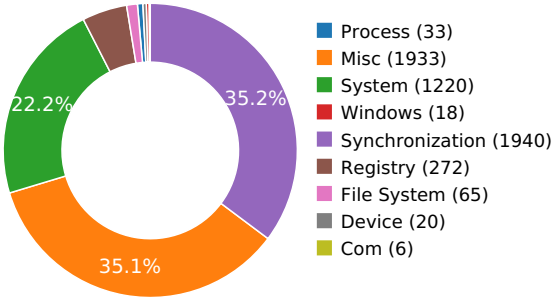


Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

The executable is compressed using UPX Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory Show sources

VALKYRIE COMODO

Behavior Graph

23:46:52 **23:46:52** **23:46:53**

PID 2876

23:46:52 **Create Process** The malicious file created a child process as c0e993fa53b4d63bf2775c9bf42027fc1257f88c.exe **(PPID 1636)**

23:46:52 NtAllocateVirtualMem

23:46:52 NtTerminateProcess

PID 1280

23:46:53 **Create Process** The malicious file created a child process as c0e993fa53b4d63bf2775c9bf42027fc1257f88c.exe **(PPID 2876)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\c0e993fa53b4d63bf2775c9bf42027fc1257f88c.ENU
C:\Users\user\AppData\Local\Temp\c0e993fa53b4d63bf2775c9bf42027fc1257f88c.ENU.DLL
C:\Users\user\AppData\Local\Temp\c0e993fa53b4d63bf2775c9bf42027fc1257f88c.EN
C:\Users\user\AppData\Local\Temp\c0e993fa53b4d63bf2775c9bf42027fc1257f88c.EN.DLL
C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Users\user\AppData\Local\Temp\c0e993fa53b4d63bf2775c9bf42027fc1257f88c.exe.Local\
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll
C:\Windows\WindowsShell.Manifest
\??\MountPointManager
C:\Users\user\AppData\Local\Temp\c0e993fa53b4d63bf2775c9bf42027fc1257f88c.exe
\Device\KsecDD

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
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
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext

RESOLVED APIS

kernel32.dll.Sleep
kernel32.dll.TlsSetValue
kernel32.dll.TlsGetValue
kernel32.dll.LocalAlloc
kernel32.dll.GetModuleHandleA
kernel32.dll.GetACP
kernel32.dll.VirtualFree
kernel32.dll.VirtualAlloc
kernel32.dll.GetTickCount
kernel32.dll.QueryPerformanceCounter
kernel32.dll.GetCurrentThreadId

kernel32.dll.InterlockedDecrement
kernel32.dll.InterlockedIncrement
kernel32.dll.VirtualQuery
kernel32.dll.WideCharToMultiByte
kernel32.dll.MultiByteToWideChar
kernel32.dll.lstrlenA
kernel32.dll.lstrcpynA
kernel32.dll.LoadLibraryExA
kernel32.dll.GetThreadLocale
kernel32.dll.GetStartupInfoA
kernel32.dll.GetProcAddress
kernel32.dll.GetModuleFileNameA
kernel32.dll.GetLocaleInfoA
kernel32.dll.GetCommandLineA
kernel32.dll.FreeLibrary
kernel32.dll.FindFirstFileA
kernel32.dll.FindClose
kernel32.dll.ExitProcess
kernel32.dll.CreateThread
kernel32.dll.CompareStringA
kernel32.dll.WriteFile
kernel32.dll.UnhandledExceptionFilter
kernel32.dll.RtlUnwind
kernel32.dll.RaiseException
kernel32.dll.GetStdHandle
kernel32.dll.lstrcpyA
kernel32.dll.WaitForSingleObject
kernel32.dll.SizeofResource
kernel32.dll.SetThreadLocale
kernel32.dll.SetFileTime
kernel32.dll.SetFilePointer
kernel32.dll.SetFileAttributesW
kernel32.dll.SetEvent
kernel32.dll.SetErrorMode
kernel32.dll.SetEndOfFile

kernel32.dll.ResetEvent
kernel32.dll.ReadFile
kernel32.dll.MulDiv
kernel32.dll.MoveFileW
kernel32.dll.LockResource
kernel32.dll.LoadResource
kernel32.dll.LoadLibraryA
kernel32.dll.LeaveCriticalSection
kernel32.dll.InitializeCriticalSection
kernel32.dll.GlobalUnlock
kernel32.dll.GlobalReAlloc
kernel32.dll.GlobalHandle
kernel32.dll.GlobalLock
kernel32.dll.GlobalFree
kernel32.dll.GlobalFindAtomA
kernel32.dll.GlobalDeleteAtom
kernel32.dll.GlobalAlloc
kernel32.dll.GlobalAddAtomA
kernel32.dll.GetVersionExA
kernel32.dll.GetVersion
kernel32.dll.GetModuleFileNameW
kernel32.dll.GetLocalTime
kernel32.dll.GetLastError
kernel32.dll.GetFullPathNameA
kernel32.dll.GetFileAttributesA
kernel32.dll.GetDiskFreeSpaceA
kernel32.dll.GetDateFormatA
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetCommandLineW
kernel32.dll.GetCPInfo

REGISTRY KEYS

HKEY_CURRENT_USER\Software\Borland\Locales
HKEY_LOCAL_MACHINE\Software\Borland\Locales
HKEY_CURRENT_USER\Software\Borland\Delphi\Locales

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\Windows Error Reporting\WMR
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\Windows Error Reporting\WMR\Disable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\MS Shell Dlg 2
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_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\SideBySide\PreferExternalManifest
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\SideBySide\AssemblyStorageRoots
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Applications\c0e993fa53b4d63bf2775c9bf42027fc1257f88c.exe
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{d35f944c-ffec-11e6-bdeb-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c4-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c5-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Data
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2\CPC\Volume\{2400a2c6-ccb0-11e5-b7bd-806e6f6e6963}\Generation
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\c0e993fa53b4d63bf2775c9bf42027fc1257f88c.exe
HKEY_LOCAL_MACHINE\Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}\Enable
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\CTF\EnableAnchorContext
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\MS Sans Serif

READ FILES

C:\Windows\Fonts\staticcache.dat
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\System32\uxtheme.dll.Config
C:\Windows\System32\uxtheme.dll
C:\Windows\winsxs\x86_microsoft.windows.common-controls_6595b64144ccf1df_6.0.7601.17514_none_41e6975e2bd6f2b2\comctl32.dll

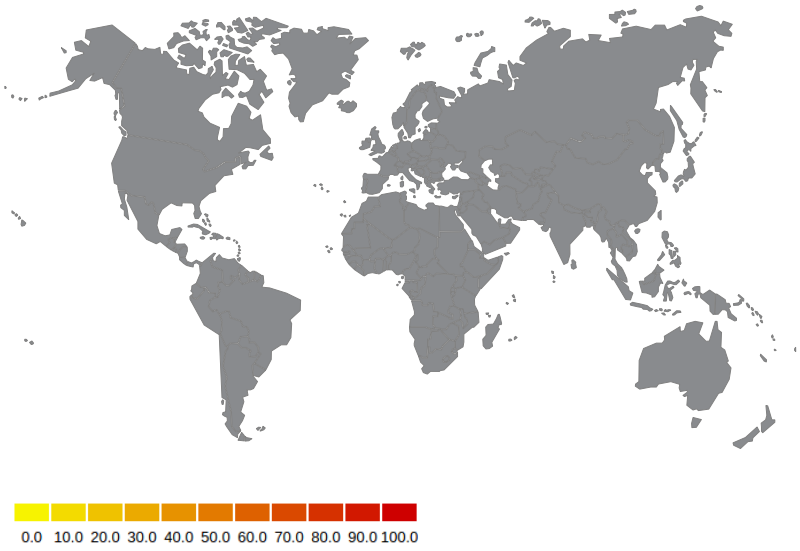
C:\Windows\WindowsShell.Manifest
\Device\KsecDD

MUTEXES

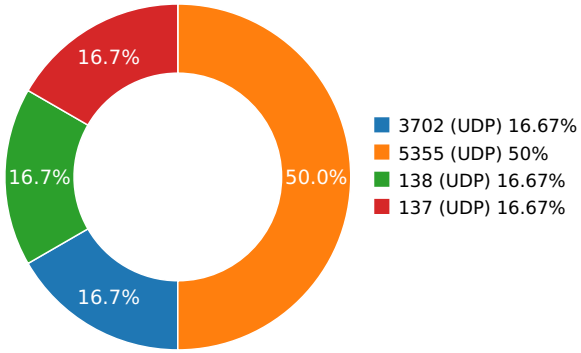
STOPSCARABSTOPSCARABSTOPSCARABSTOPSCARABSTOPSCARAB
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

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
3.09226608276	Sandbox	224.0.0.252	5355
3.10503196716	Sandbox	224.0.0.252	5355
3.11939501762	Sandbox	239.255.255.250	3702
3.12012386322	Sandbox	192.168.56.255	137
5.66720604897	Sandbox	224.0.0.252	5355
6.80902194977	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:	decrypter.exe
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows, UPX compressed
SHA1:	c0e993fa53b4d63bf2775c9bf42027fc1257f88c
MD5:	8932a7c2d3d33c5fe46252f3c8713696
First Seen Date:	2018-06-23 13:32:54.037060 (6 months ago)
Number Of Clients Seen:	3
Last Analysis Date:	2018-06-23 13:32:54.037060 (6 months ago)
Human Expert Analysis Result:	No human expert analysis verdict given to this sample yet.

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	3
Trid	[]
Compilation Time Stamp	0x5A140888 [Tue Nov 21 11:05:44 2017 UTC]
Entry Point	0x4a9da0 (UPX1)
Machine Type	Intel 386 or later - 32Bit
File Size	290304
Ssdeep	
Sha256	878b796cfa0bd62455381c0e0ac3f22056b2e34e8cccb5144337ad463fb851af
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
UPX0	0x1000	0x6e000	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
UPX1	0x6f000	0x3b000	0x3b000	7.92456441225	42e179451426485b75311904c575e462
.rsrc	0xaa000	0xc000	0xba00	5.6576383326	b50072582ec25633c70eb6957671664f

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 699204, u'sha256': u'b8e6fc93d423931acbddae3c27dd3c4eb2a394005d746951a971cb700e0ee510', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 699516, u'sha256': u'ce19ace18e87b572e6912306776226af5b8e63959c61cde70a8ff05b3bbdcc41', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 699828, u'sha256': u'ee1c9c194199c320c893b367602ccc7ee7270bd4395d029f727e097634f47f8c', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 700140, u'sha256': u'9d9edf87ca203ecc60b246cc783d54218dd0ce77d3a025d0bafc580995a4abd8', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 700452, u'sha256': u'99676c52310db365580965ea646ece86c62951bfd97ec0aae9f738a202a90593', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 700764, u'sha256': u'11726dcf1eebe23a1df5eb0ee2af39196b702eddd69083d646e4475335130b28', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_CURSOR', u'offset': 701076, u'sha256': u'6f938aab0a03120de4ef8b27aff6ba5146226c92a056a6f04e5ec8d513ce5f9d', u'type': u'data', u'size': 308}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 701388, u'sha256': u'c0ede68a98bd2bc58c78564dfb42f1640dc29766d3ab2782ab8b5ed28c6fd414', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 701856, u'sha256':

u'46cfc44afa8ab31ae3da35fa8346e4c085c441659d9992b09fc8ad517f2b289a', u'type': u'data', u'size': 484}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 702344, u'sha256': u'c0ede68a98bd2bc58c78564dfb42f1640dc29766d3ab2782ab8b5ed28c6fd414', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 702812, u'sha256': u'f8e1696801fe89b88936ac4226cea03bfa5aa345aa33ca982822ae7fbc6557e2', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 703280, u'sha256': u'cb7421b5c6af74c3159c361f3bb78bba8a488d8979d1250e106fa96cbf928789', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 703748, u'sha256': u'41f05a4df5f42d92b879493d51941de342d36460fe15c0f3b63b2b706b928fef', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 704216, u'sha256': u'81265e63c89ee5c2e5126452e22f84e9be9452449f3e5959ab6d346cb58b2bde', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 704684, u'sha256': u'6b97877cdd547e6ba6467f86055f1fc7b06660b034439f0da4c137538ef14a83', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 705152, u'sha256': u'c925e4a8cbf6d42dbb1220a510614df725558f8d843338982bab8c4e020f6429', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 705620, u'sha256': u'6b97877cdd547e6ba6467f86055f1fc7b06660b034439f0da4c137538ef14a83', u'type': u'data', u'size': 464}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_BITMAP', u'offset': 706088, u'sha256': u'78507a772de646626b196a743cee75b298a68c33a0fd482842071519d59037b2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 232}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_ICON', u'offset': 706324, u'sha256': u'0a35659a2ebd558d223a4192ebe2e6ccb3e652b4530c209a78996fcfd6ac7657', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_ICON', u'offset': 715968, u'sha256': u'69cb2cd70bf4e2dc49fc0c9dcddf1634048dc509e33c782fe8ac846c82e56bfa', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 720236, u'sha256': u'771f64afb45a9edc8c4f6c5b2039f9b32623cea53bf0cab5bf1f371cc5d1abe4', u'type': u'data', u'size': 82}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_DIALOG', u'offset': 720324, u'sha256': u'26be3f5d9e8788884e3d857861b2666da59e7e80dfaa6e7e52832428980204fc', u'type': u'data', u'size': 82}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 720412, u'sha256': u'66bce5bf011accb6bba8df8a2e24c74157519acb74ed44f0f9e6fb2c4a2219ff', u'type': u'data', u'size': 160}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 720576, u'sha256': u'18f023ca72b91d9141f342e0a32879c2be09e70534c24475286c3e21f8f97d04', u'type': u'data', u'size': 900}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 721480, u'sha256': u'1c01171aff3d3f6ac787048b7e27125a92438141baae300f6f74738a6e5c8cb7', u'type': u'Hitachi SH big-endian COFF object, not stripped', u'size': 256}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 721740, u'sha256': u'c7e93652bf50229b89e363c92b6668d0c6547e6f539ad5352393cebb0a15d69a', u'type': u'data', u'size': 204}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 721948, u'sha256': u'690d40c14621ca430796ac86f75122bcc98ec1938610eee12f2a476a65feb70a', u'type': u'data', u'size': 272}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 722224, u'sha256': u'ffd9b056960ea522c3f93d0a883c880b646cc6012dc6153f896d3a06a01671e8', u'type': u'data', u'size': 1036}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 723264, u'sha256': u'3b1f89d98d3ef7ab26a63745130ad46c5773496cf6f47ceab77cc291e47b9cd8', u'type': u'data', u'size': 916}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 724184, u'sha256': u'd6bcdff73ced352f6a37135ba149af7160dd8f3a01efa92505af4b7a3c5377dd', u'type': u'data', u'size': 904}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 725092, u'sha256': u'dc60627c4638683ea9b0874a7fd61373112398bc637687aa42b97ba1b14c04ef', u'type': u'data', u'size': 1008}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 726104, u'sha256': u'367dfc77d6f740d954f9073067dc8c668d29c64af6cc3dc003f66781c907764b', u'type': u'data', u'size': 400}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 726508, u'sha256': u'07a699dfba3b6f2e997c6ee78a0e0e1dad18c948aff0f1767b28f5ee6e41fdc3', u'type': u'data', u'size': 204}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 726716, u'sha256': u'd14cf3dfe03eb5e1d1dea9dae8c3716c41107979ddf121a7be2560f39c5385f3', u'type': u'data', u'size': 452}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 727172, u'sha256': u'6b96d88f3182ca0a51213c6378b452178c3d17ab9eb99516f862f306a1efe878', u'type': u'data', u'size': 980}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 728156, u'sha256': u'190ded281b8e85f67de35d162aaf032712b956ce4e30184c870749e11309a7c5', u'type': u'data', u'size': 800}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 728960, u'sha256': u'407743f3bfd7bdf398a523a3c844fb0857f6564fdd87e718b45765624e4ae688', u'type': u'data', u'size': 672}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 729636, u'sha256': u'b9304cdb22015513e72a52c9950bc2439e4c8ccc13fb3f568da3a07203f5d299', u'type': u'ASCII text, with no line terminators', u'size': 180}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 729820, u'sha256': u'e7dbe99baa5c1045cdf7004edb037018b2e0f639a5edcf800ec4514d5c8e35b5', u'type': u'data', u'size': 16}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 729840, u'sha256': u'd9e052861281898874783 71d4241aec0a1318b01f89c6a4d17a0369d86504cb3', u'type': u'data', u'size': 788}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_RCDATA', u'offset': 730632, u'sha256': u'9855ca38b6f5f0062040ce55fe7ac85599aa462c715f08efd4f31bae53611b3b', u'type': u"Delphi compiled form 'TForm_Decrypter'", u'size': 12260}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 742896, u'sha256': u'c53efa8085835ba129c1909beaff8a67b45f50837707f22dfff0f24d8cd26710', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 742920, u'sha256': u'b07e022f8ef0a8e5fd3f56986b2e5bf06df07054e9ea9177996b0a6c27d74d7c', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 742944, u'sha256': u'43f40dd5140804309a4c901ec3c85b54481316e67a6fe18beb9d5c0ce3a42c3a', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 742968, u'sha256': u'ff47a48c11c234903a7d625cb8b62101909f735ad84266c98dd4834549452c39', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 742992, u'sha256': u'a0adcedb82b57089f64e2857f97cefd6cf25f4d27eefc6648bda83fd5fef66bb', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 743016, u'sha256': u'6e1e7738a1b6373d8829f817915822ef415a1727bb5bb7cfe809e31b3c143ac5', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

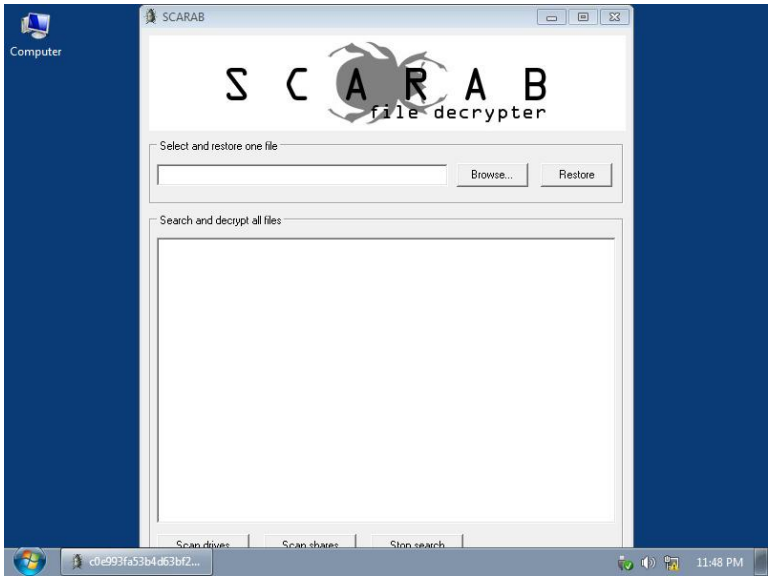
{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_CURSOR', u'offset': 743040, u'sha256': u'326c048595bbc72e3f989cb3b95fbf09dc83739ced3cb13eb6f03336f95d74f1', u'type': u'MS Windows cursor resource - 1 icon, 32x256, hotspot @1x1', u'size': 20}

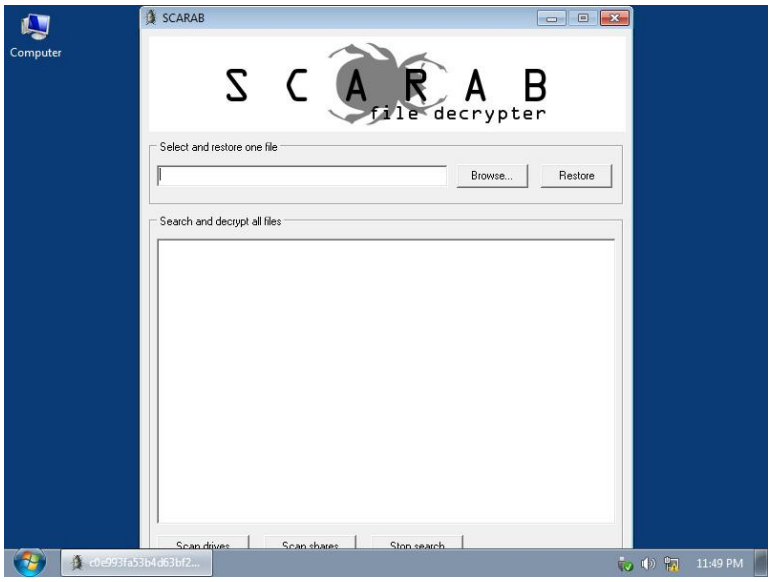
{u'lang': u'LANG_RUSSIAN', u'name': u'RT_GROUP_ICON', u'offset': 743064, u'sha256': u'e2f348c219d2ec9efed64e62c0c8a7fcaeeb8aa63afa561650684b95c335ee57', u'type': u'MS Windows icon resource - 2 icons, 48x48', u'size': 34}

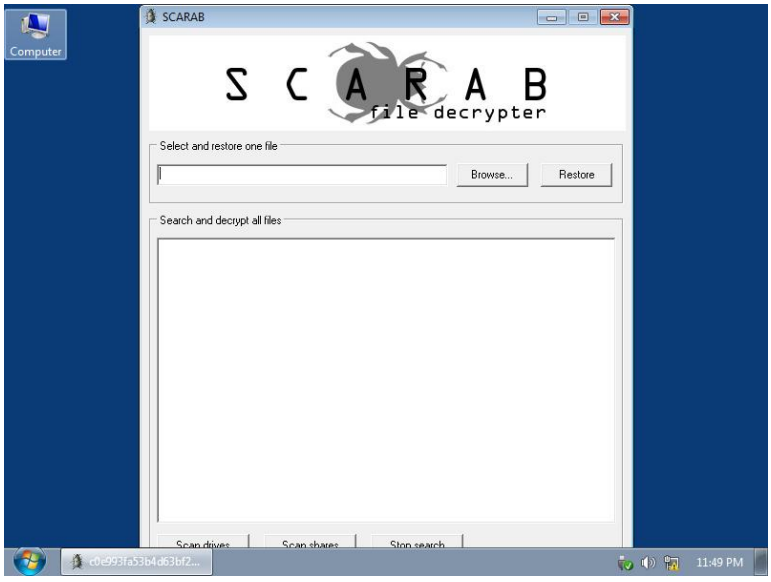
CERTIFICATE VALIDATION

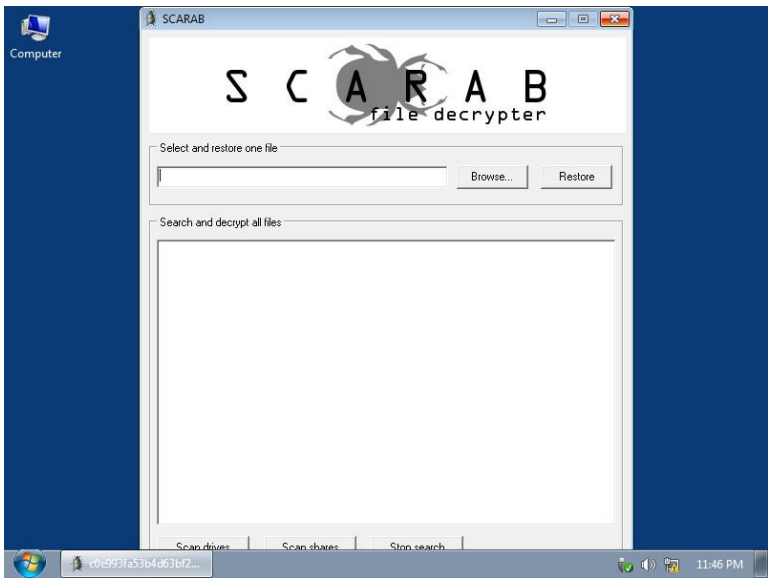
- Certificate Validation is not Applicable ?

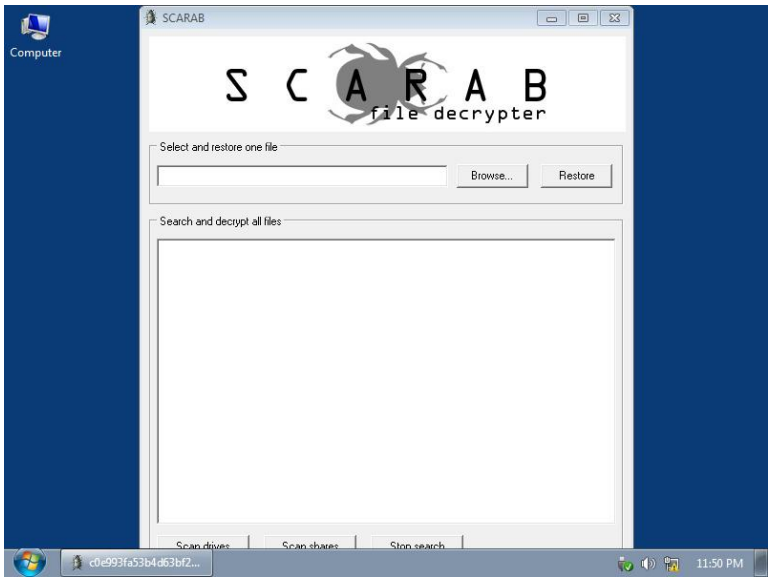
SCREENSHOTS

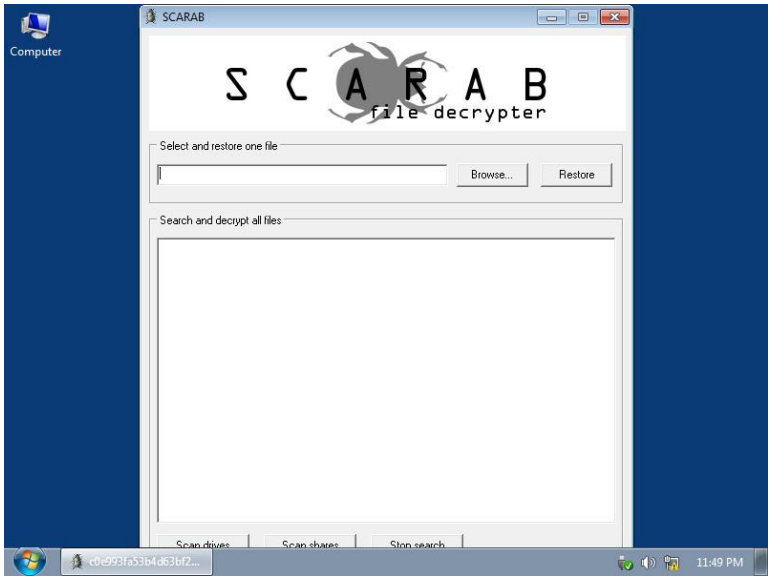


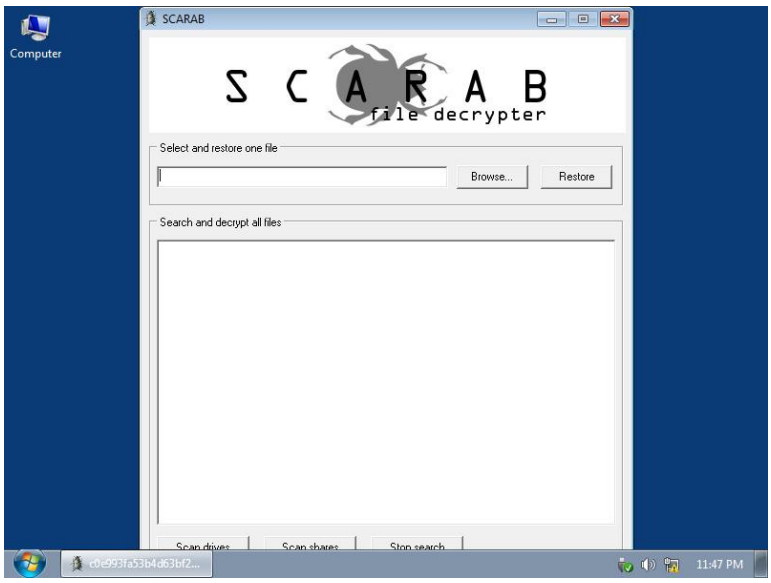

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
11:49 PM

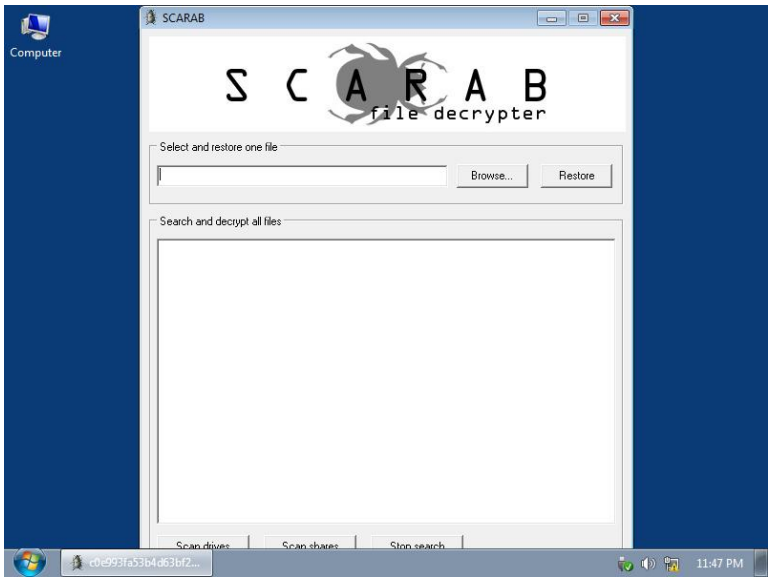

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
11:49 PM

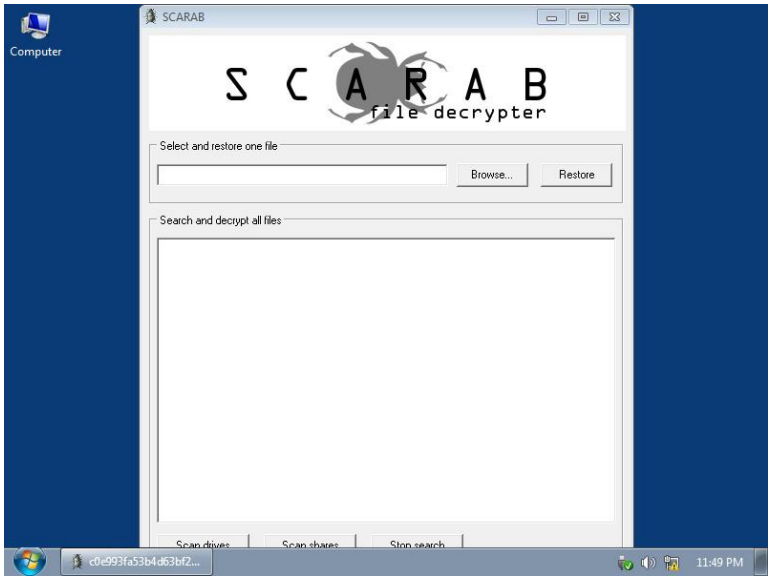

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
11:46 PM

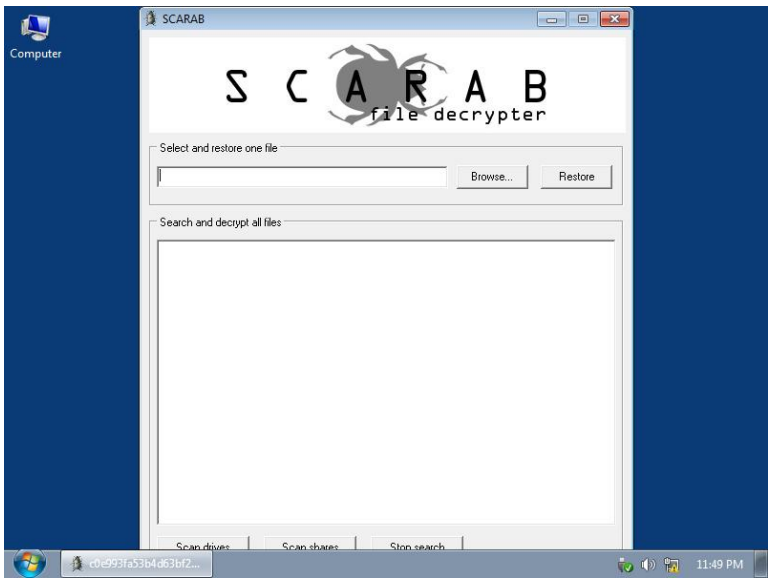

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:50 PM

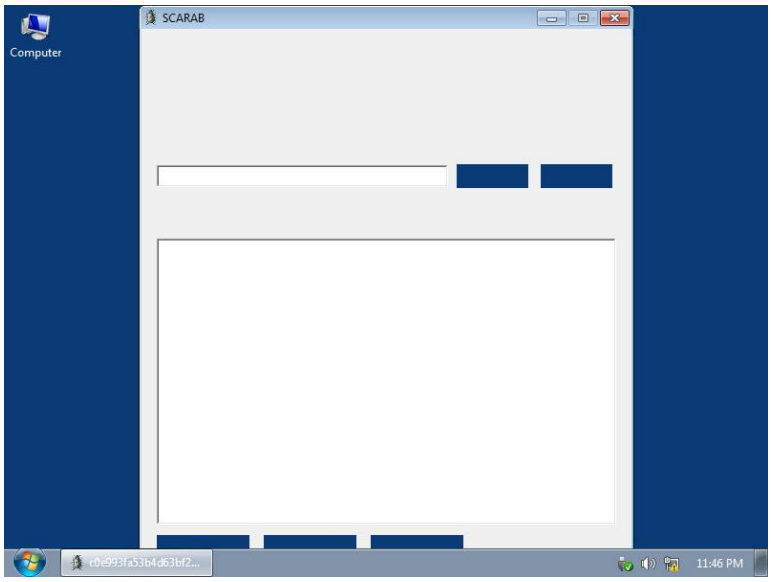

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:49 PM


Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:47 PM

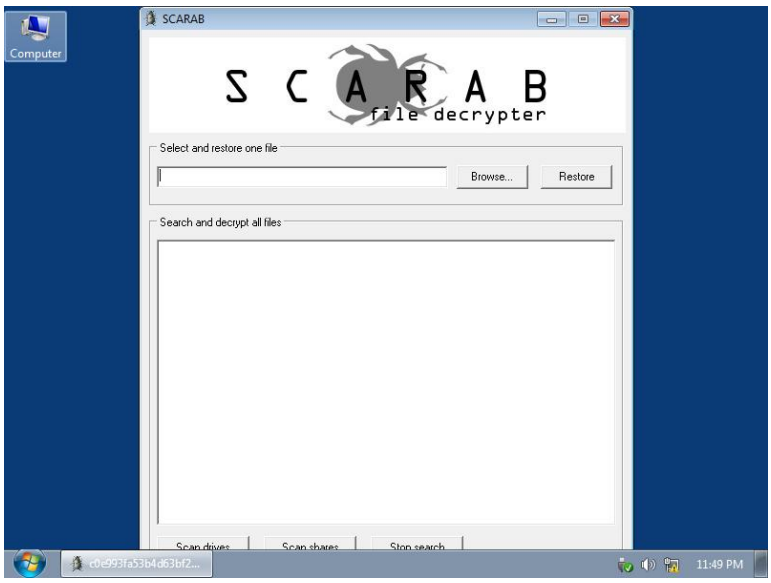

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:47 PM

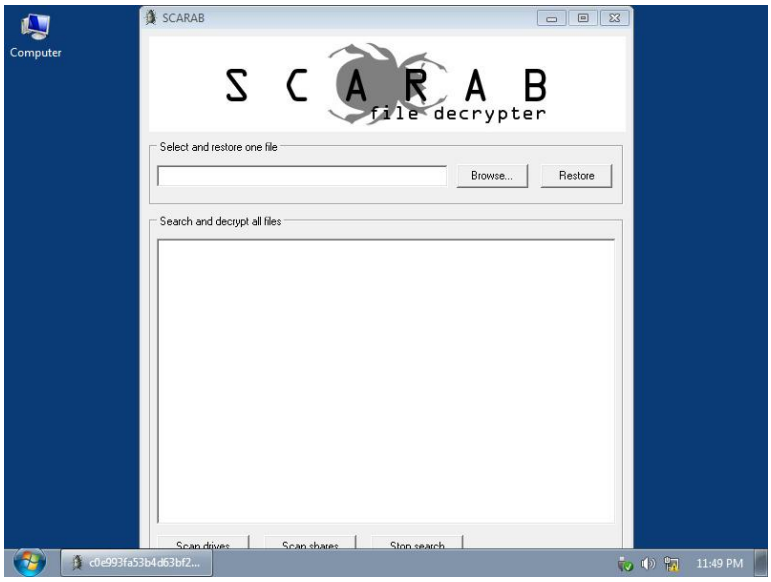

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:49 PM

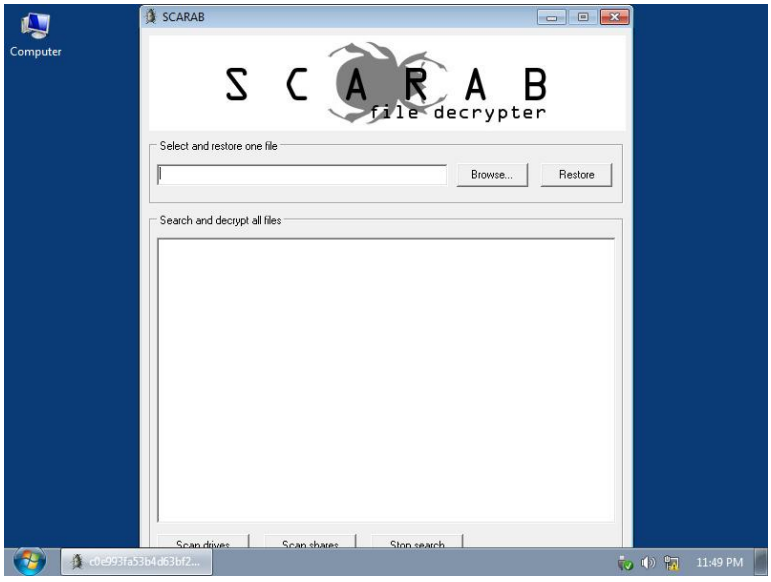

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:49 PM

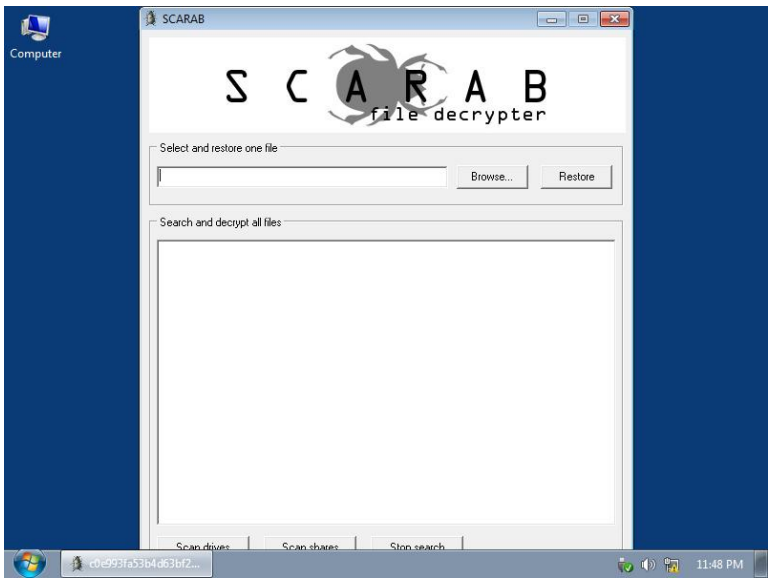

Computer
SCARAB
11:46 PM

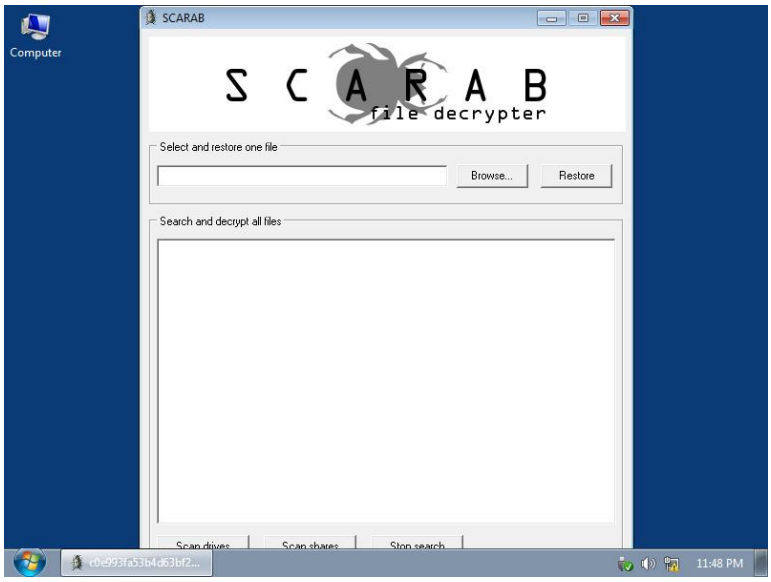

Computer
11:46 PM

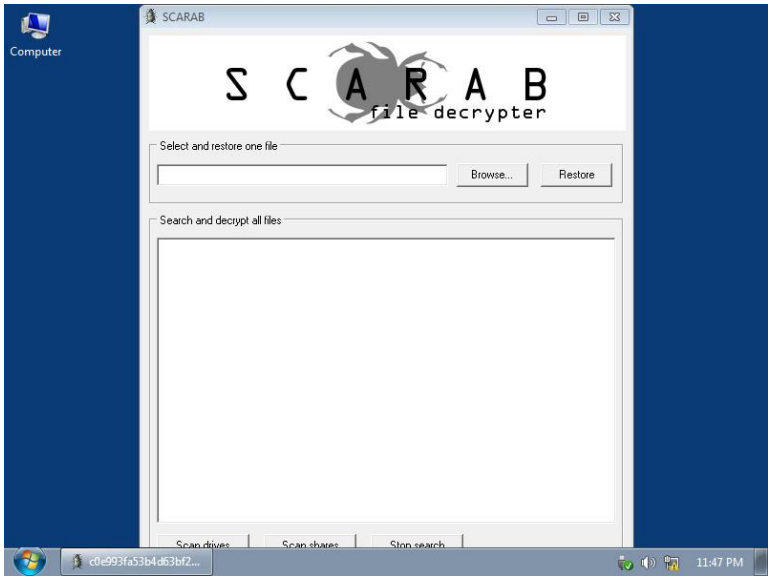

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
11:49 PM

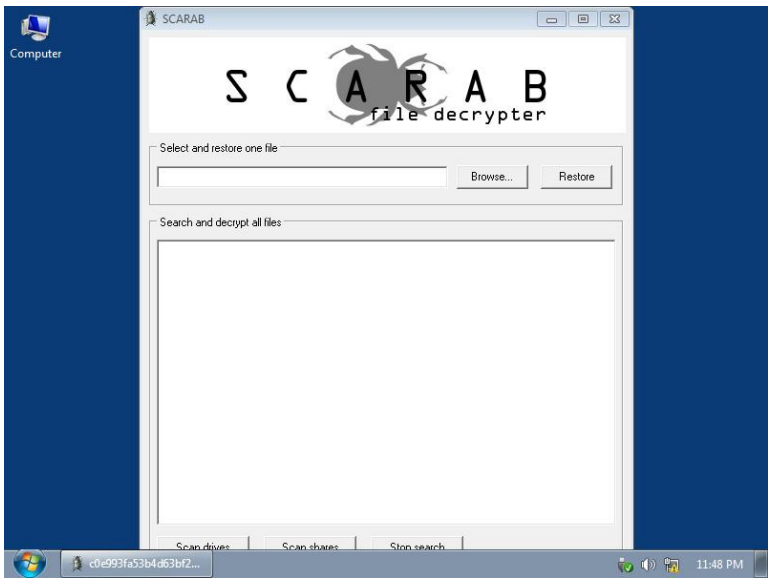

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:49 PM

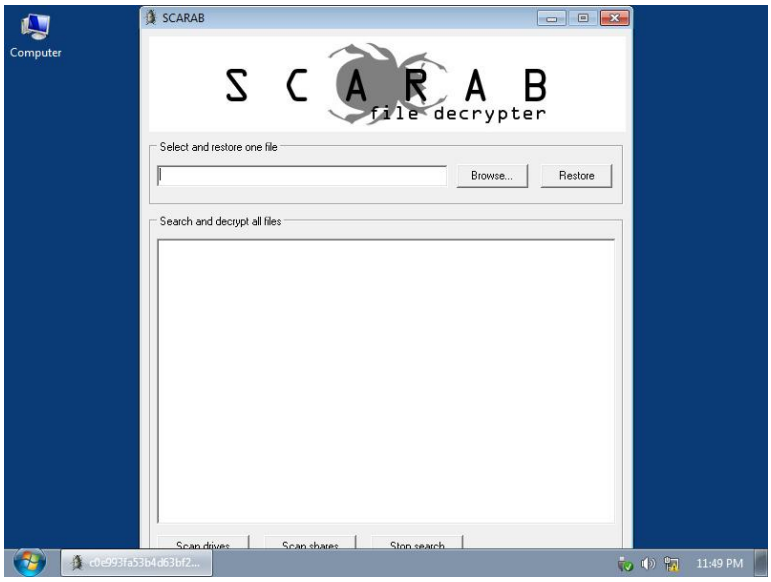

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:49 PM

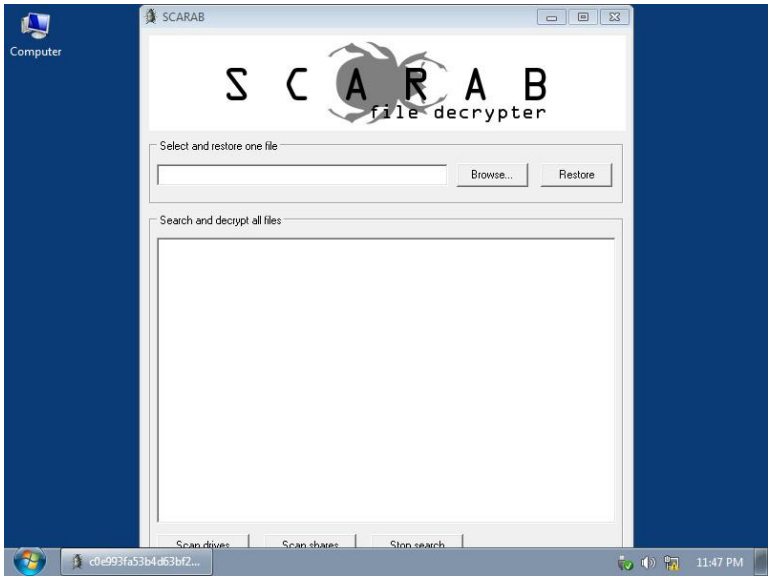

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:48 PM

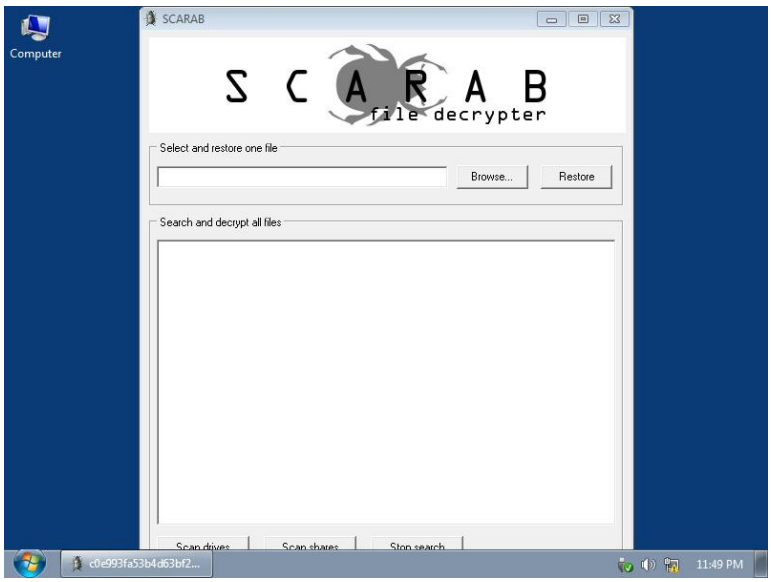

Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:48 PM


Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:47 PM


Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:48 PM


Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:49 PM


Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:47 PM


Computer
SCARAB
S C A R A B
file decrypter
Select and restore one file
Browse...
Restore
Search and decrypt all files
Scan drives
Scan shares
Stop search
c0e993fa53b4d63bf2...
11:49 PM