Summary

File Name: ThreatHunterAssessmentTool.exe

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

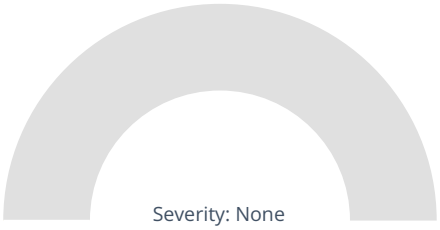
SHA1: 946f4f8b40fefac6f03c78bbed794b3c118d7f8b

MD5: d9bf14670243c18c8a52ecfd65a65ace

CLEAN

Xcitium Verdict Cloud Final Verdict

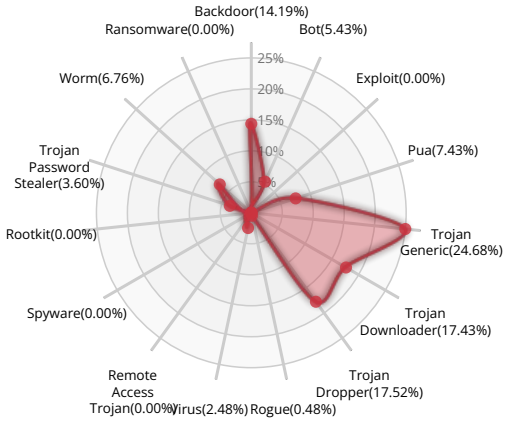
DETECTION SECTION



Severity: None

Verdict: Clean

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION

ACTIVITY OVERVIEW

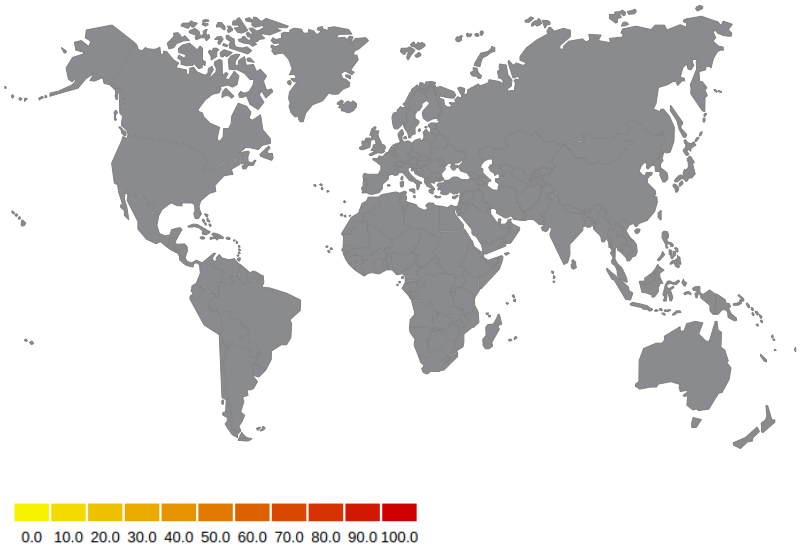
Activity Details

Behavior Graph

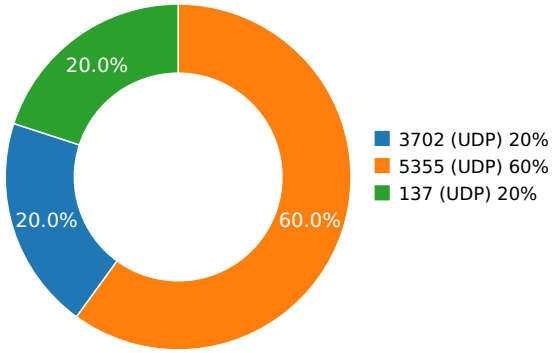
Behavior Summary

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
3.0082719326	Sandbox	224.0.0.252	5355
3.17472195625	Sandbox	192.168.56.255	137
3.178429842	Sandbox	224.0.0.252	5355
3.86015796661	Sandbox	239.255.255.250	3702
5.7383890152	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:	ThreatHunterAssessmentTool.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	946f4f8b40fefac6f03c78bbed794b3c118d7f8b
MD5:	d9bf14670243c18c8a52ecfd65a65ace
First Seen Date:	2023-06-12 16:31:31.700910 (4 months ago)
Number Of Clients Seen:	12
Last Analysis Date:	2023-07-11 09:43:33.256623 (3 months ago)
Human Expert Analysis Date:	2023-06-12 21:52:44.002037 (4 months ago)
Human Expert Analysis Result:	Clean

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	4
Trid	[[33.6, u'OS/2 Executable (generic)'], [33.1, u'Generic Win/DOS Executable'], [33.1, u'DOS Executable Generic']]
Compilation Time Stamp	0x4DB951AC [Thu Apr 28 11:38:20 2011 UTC]
LegalCopyright	Copyright \xa9 2018 Comodo
InternalName	7zS.sfx
FileVersion	6.0.0.0
CompanyName	Xcitium
ProductName	THAT
ProductVersion	6.0.0.0
FileDescription	Threat Hunter Assessment Tool
OriginalFilename	THAT.exe
Translation	0x0409 0x04b0
Entry Point	0x4121cf (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	13661336
Ssdeep	393216:cMIlREOTIqI8B9iykrdVaR9ORrWMp+o6dBS:6lmOcqI+irSa457
Sha256	3c58ae6738754da759ca8f548d382147dacedb431c35250a9ce7c2af8ff1b92b
Exifinfo	[{u'EXE:FileSubtype': 0, u'File:FilePermissions': u'rw-r--r--', u'SourceFile': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/4/6/f/946f4f8b40fefac6f03c78bbed794b3c118d7f8b', u'EXE:OriginalFileName': u'THAT.exe', u'EXE:ProductName': u'THAT', u'EXE:InternalName': u'7zS.sfx', u'File:MIMEType': u'application/octet-stream', u'File:FileAccessDate': u'2023:07:11 09:43:14+00:00', u'EXE:InitializedDataSize': 81408, u'File:FileModifyDate': u'2023:07:11 09:40:53+00:00', u'EXE:FileVersionNumber': u'1.2.11222.1', u'EXE:FileVersion': u'6.0.0.0', u'File:FileSize': u'13 MB', u'EXE:CharacterSet': u'Unicode', u'EXE:MachineType': u'Intel 386 or later, and compatibles', u'EXE:FileOS': u'Windows NT 32-bit', u'EXE:ProductVersion': u'6.0.0.0', u'EXE:ObjectFileType': u'Executable application', u'File:FileType': u'Win32 EXE', u'EXE:CompanyName': u'Xcitium', u'File:FileName': u'946f4f8b40fefac6f03c78bbed794b3c118d7f8b', u'EXE:ImageVersion': 0.0, u'File:FileTypeExtension': u'exe', u'EXE:OSVersion': 4.0, u'EXE:PEType': u'PE32', u'EXE:TimeStamp': u'2011:04:28 11:38:20+00:00', u'EXE:FileFlagsMask': u'0x003f', u'EXE:LegalCopyright': u'Copyright \xa9 2018 Comodo', u'EXE:LinkerVersion': 8.0, u'EXE:FileFlags': u'(none)', u'EXE:Subsystem': u'Windows GUI', u'File:Directory': u'/nfs/fvs/valkyrie_shared/core/valkyrie_files/9/4/6/f', u'EXE:FileDescription': u'Threat Hunter Assessment Tool', u'EXE:EntryPoint': u'0x121cf', u'EXE:SubsystemVersion': 4.0, u'EXE:CodeSize': 71680, u'File:FileInodeChangeDate': u'2023:07:11 09:40:54+00:00', u'EXE:UninitializedDataSize': 0, u'EXE:LanguageCode': u'English (U.S.)', u'ExifTool:ExifToolVersion': 10.1, u'EXE:ProductVersionNumber': u'1.2.11222.1'}]
Mime Type	application/x-dosexec
Imphash	c769210c368165fcb9c03d3f832f55eb

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x11713	0x11800	6.60951084962	a33aa34b7879bccd6f1864408fd68dcf
.rdata	0x13000	0x30ee	0x3200	5.5403621921	007197a7f03fd570aac173835b4d4e9d
.data	0x17000	0x292c	0x800	3.63946504735	9627e4496a259b33307cd6b8b9dae798
.rsrc	0x1a000	0x103ad	0x10400	6.56769990471	b79b47f5adc02eae4a1c9647a11e5ab5

PE Imports

- COMCTL32.dll
  - None
- SHELL32.dll
  - SHGetSpecialFolderPathW
  - ShellExecuteExW
  - SHGetMalloc
  - SHGetPathFromIDListW
  - SHBrowseForFolderW
  - SHGetFileInfoW
  - ShellExecuteW
- GDI32.dll
  - CreateFontIndirectW
  - DeleteObject
  - GetDeviceCaps
  - GetObjectW
  - CreateCompatibleDC
  - SelectObject
  - CreateCompatibleBitmap
  - SetStretchBltMode
  - DeleteDC
  - GetCurrentObject
  - StretchBlt
- USER32.dll
  - GetWindowRect
  - ScreenToClient
  - CreateWindowExW
  - GetWindowTextW
  - GetMessageW
  - GetParent
  - KillTimer
  - DestroyWindow
  - CharUpperW
  - EndDialog
  - SendMessageW
  - wsprintfW
  - CopyImage
  - ReleaseDC
  - GetWindowDC
  - SetWindowPos
  - GetMenu
  - GetWindowLongW
  - DispatchMessageW
  - GetWindowTextLengthW
  - GetSysColor
  - SetWindowTextW
  - MessageBoxA
  - wsprintfA
  - GetKeyState
  - GetDlgItem
  - GetClientRect
  - GetSystemMetrics
  - SetWindowLongW
  - SetFocus
  - SystemParametersInfoW
  - ShowWindow
  - DrawTextW
  - GetDC
  - ClientToScreen

    - GetWindow
    - DialogBoxIndirectParamW
    - DrawIconEx
    - CallWindowProcW
    - DefWindowProcW
    - IsWindow
    - wvsprintfW
    - LoadImageW
    - LoadIconW
    - MessageBeep
    - EnableWindow
    - EnableMenuItem
    - GetSystemMenu
    - GetClassNameA
    - SetTimer
- ole32.dll
    - CreateStreamOnHGlobal
    - CoCreateInstance
    - CoInitialize
- OLEAUT32.dll
    - SysAllocString
    - VariantClear
    - OleLoadPicture
- KERNEL32.dll
    - SetEndOfFile
    - EnterCriticalSection
    - LeaveCriticalSection
    - WaitForMultipleObjects
    - DeleteCriticalSection
    - GetModuleHandleA
    - SetFileTime
    - ReadFile
    - SetFilePointer
    - GetFileSize
    - GetSystemDirectoryW
    - FormatMessageW
    - lstrcpyW
    - LocalFree
    - IsBadReadPtr
    - SuspendThread
    - ResumeThread
    - TerminateThread
    - InitializeCriticalSection
    - ResetEvent
    - SetEvent
    - CreateEventW
    - GetVersionExW
    - GetCommandLineW
    - GetModuleFileNameW
    - SetCurrentDirectoryW
    - GetDriveTypeW
    - CreateFileW
    - CloseHandle
    - SetEnvironmentVariableW
    - GetTempPathW
    - lstrlenW
    - GetSystemTimeAsFileTime
    - CompareFileTime
    - SetThreadLocale
    - FindFirstFileW
    - DeleteFileW
    - FindNextFileW
    - FindClose
    - RemoveDirectoryW
    - ExpandEnvironmentStringsW
    - WideCharToMultiByte
    - VirtualAlloc
    - GlobalMemoryStatusEx
    - lstrcmpW
    - GetEnvironmentVariableW
    - lstrcmpiW
    - lstrlenA
    - GetLocaleInfoW
    - MultiByteToWideChar
    - GetUserDefaultUILanguage

    - GetSystemDefaultUILanguage
    - GetSystemDefaultLCID
    - lstrcmpiA
    - GlobalAlloc
    - GlobalFree
    - MulDiv
    - FindResourceExA
    - SizeofResource
    - LoadResource
    - LockResource
    - LoadLibraryA
    - GetProcAddress
    - GetModuleHandleW
    - VirtualFree
    - GetStdHandle
    - ExitProcess
    - lstrcatW
    - GetDiskFreeSpaceExW
    - SetFileAttributesW
    - SetLastError
    - Sleep
    - GetExitCodeThread
    - WaitForSingleObject
    - CreateThread
    - GetLastError
    - SystemTimeToFileTime
    - GetLocalTime
    - GetFileAttributesW
    - CreateDirectoryW
    - WriteFile
    - GetStartupInfoA
- MSVCRT.dll
    - ??2@YAPAXI@Z
    - _purecall
    - memcmp
    - free
    - memcpy
    - _controlfp
    - _except_handler3
    - __set_app_type
    - __p__fmode
    - __p__commode
    - _adjust_fdiv
    - __setusermatherr
    - _initterm
    - __getmainargs
    - _acmdln
    - exit
    - _XcptFilter
    - _exit
    - ??1type_info@@UAE@XZ
    - _onexit
    - __dllonexit
    - _CxxThrowException
    - _beginthreadex
    - _EH_prolog
    - ?_set_new_handler@@YAP6AHI@ZP6AHI@Z@Z
    - memset
    - _wcsnicmp
    - strncmp
    - malloc
    - memmove
    - _wtol
    - ??3@YAXPAX@Z

PE Resources

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 107160, u'sha256': u'a494cedff6bf53ef84409b3f6014665ac78d28d9b18b0d33fffda68f8be69577', u'type': u'PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced', u'size': 27689}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 134852, u'sha256': u'0d7345a77337839bc1402ed7a197617fdb175b34a9f78b6c8915fefacf75a839', u'type': u'dBase IV DBT of \\200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295', u'size': 16936}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 151788, u'sha256': u'45acf956885d94e3fa1a8714750c941d5baa5e5773e03aae00800a2eccdb8885', u'type': u'data', u'size': 9640}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 161428, u'sha256': u'318d15491dcecca3450de8659936ae9bbd675bb67932f5135b46617598475756', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 165692, u'sha256': u'33c7c05283d20372138b3a2270bc7172698dbed2276321181c9ae3d2ed92ac81', u'type': u'data', u'size': 2440}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 168132, u'sha256': u'a40f53de4a10bfea973fd7ab1c49b5e73c20a90d8dd819cb71b99825f0eb3f8d', u'type': u'data', u'size': 1720}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_ICON', u'offset': 169852, u'sha256': u'8feae5c40ed2714ee5d428b5f3df1ac1622bdec4164e8ef2a80f860bce61f02a', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_DIALOG', u'offset': 170980, u'sha256': u'a43e7439e0ff39f3a1beeb5485ce73b7bc7bbb071c85bdf64aa89eeccf83bf18', u'type': u'data', u'size': 336}

{u'lang': u'LANG_ENGLISH', u'name': u'RT_GROUP_ICON', u'offset': 171316, u'sha256': u'88697454a1db97b1d51cc125780faf4f6c10e30ca0947dfe5efef38b216480c5', u'type': u'MS Windows icon resource - 7 icons, 256x256', u'size': 104}

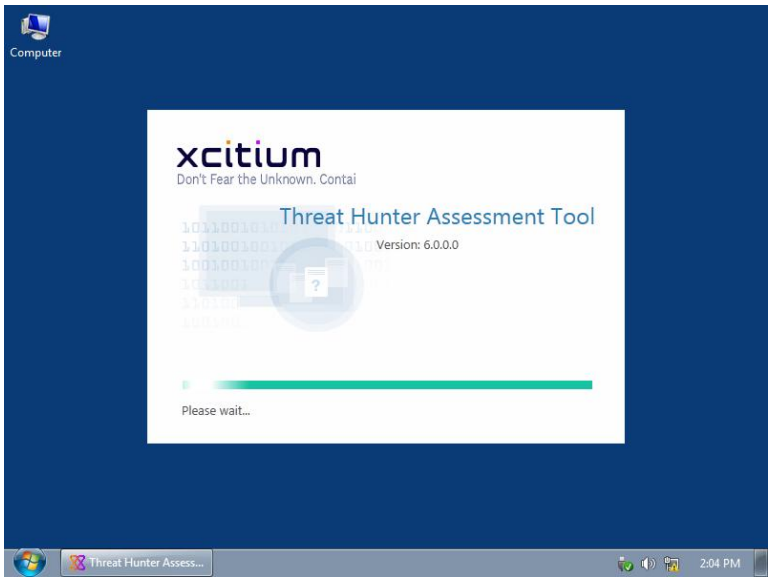
{u'lang': u'LANG_ENGLISH', u'name': u'RT_VERSION', u'offset': 171420, u'sha256': u'7b89705ffa1b74ab0e1416288ae9cd67c58830fde640475bd7f66d02cc8c1622', u'type': u'data', u'size': 704}

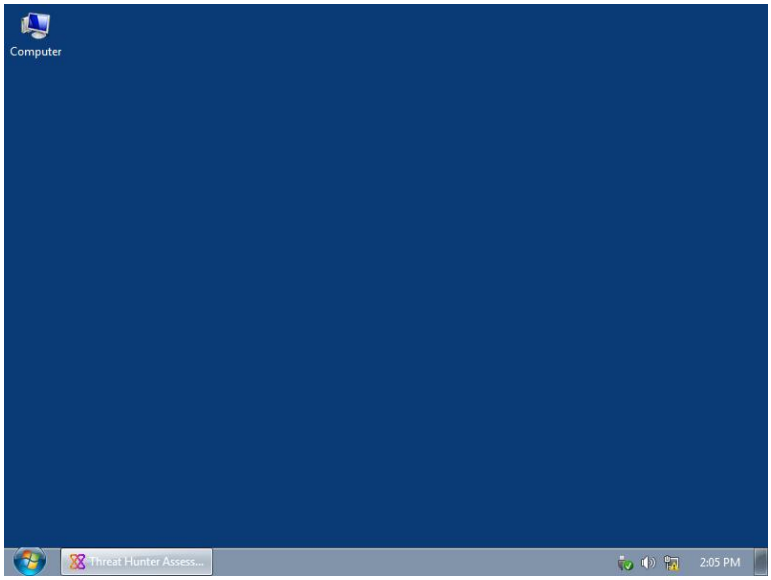
{u'lang': u'LANG_ENGLISH', u'name': u'RT_MANIFEST', u'offset': 172124, u'sha256': u'11d87b20e1bab8e3afa08d86c3ddb9bac0fa1a238c4882096432125fcc27a3a6', u'type': u'ASCII text, with CRLF line terminators', u'size': 849}

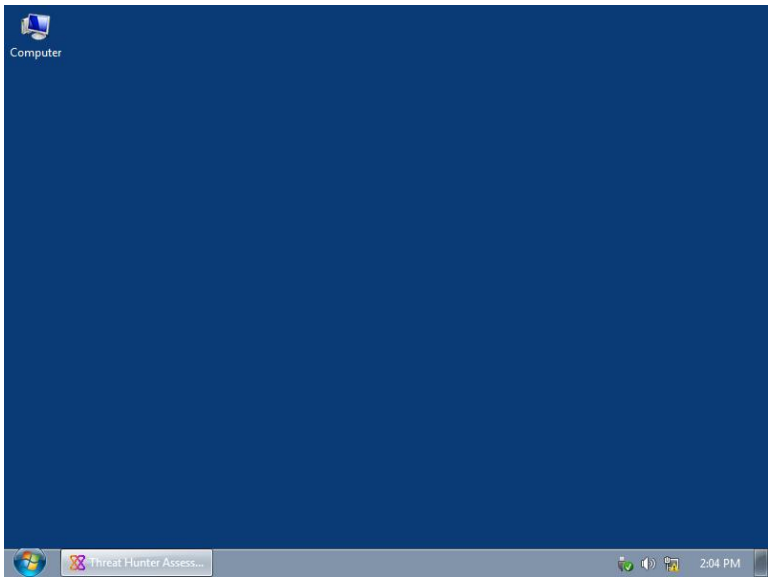
CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

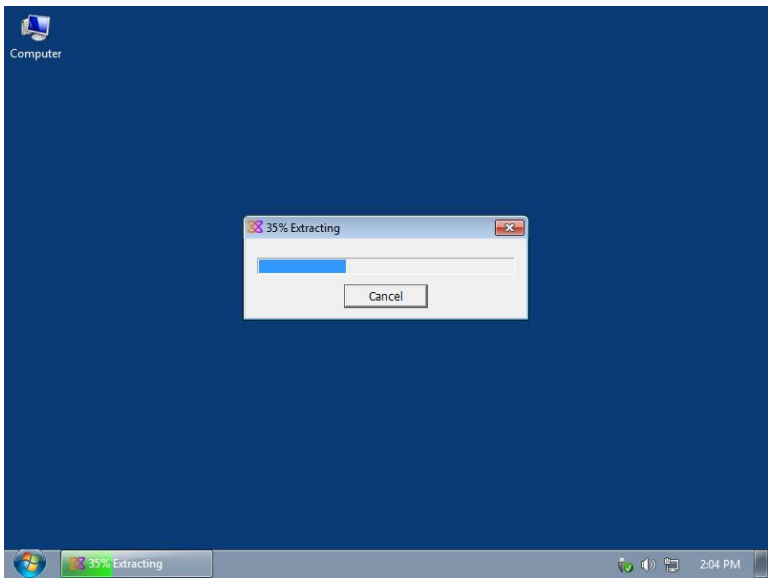
SCREENSHOTS

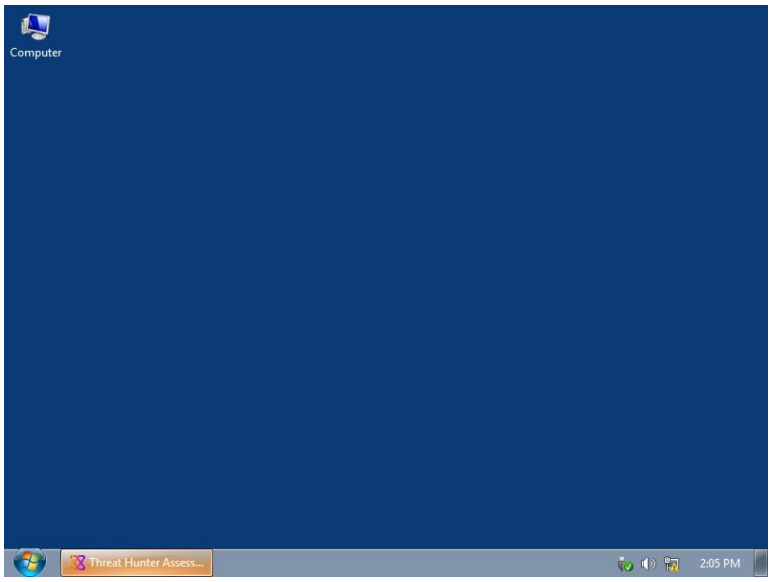


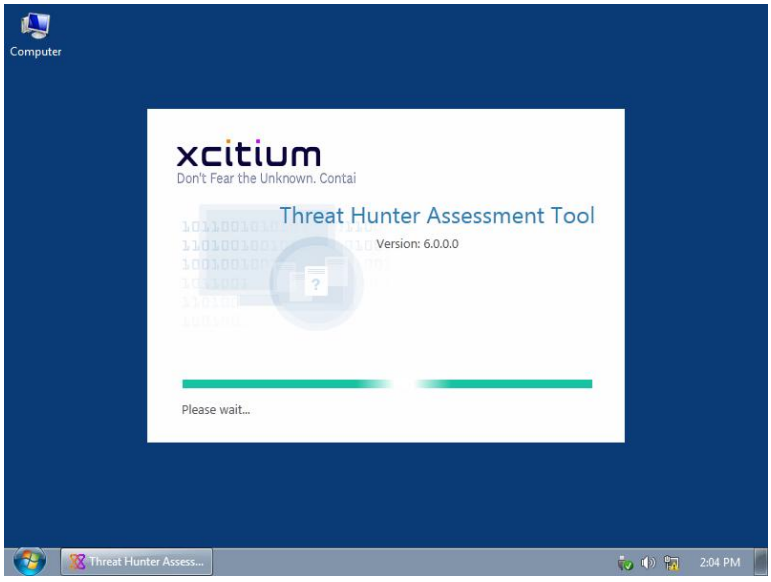



Computer
Threat Hunter Assess...
2:04 PM


Computer
2:04 PM


Computer
35% Extracting
Cancel
35% Extracting
2:04 PM


Computer
Threat Hunter Assess...
2:05 PM


Computer
xcitium
Don't Fear the Unknown. Contai
Threat Hunter Assessment Tool
Version: 6.0.0.0
Please wait...
Threat Hunter Assess...
2:04 PM