VALKYRIE COMODO

Summary

File Name: clt.exe

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

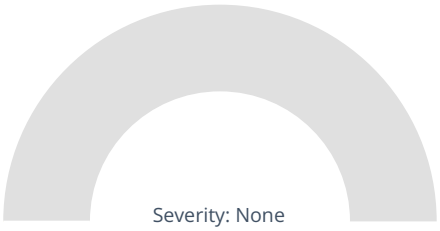
SHA1: 519c595797b293f4977654c8c61ae80dc735b703

MD5: db74dd8cfe19e770a65baade28b7bdf1

CLEAN

Valkyrie Final Verdict

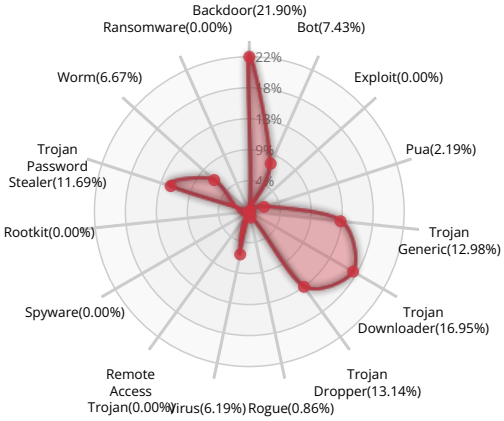
DETECTION SECTION



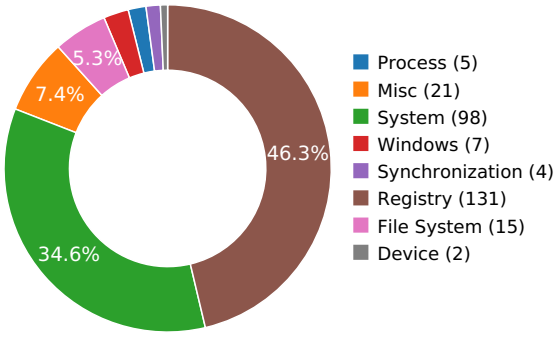
Severity: None

Verdict: Clean

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW

Packer 1 (100.00%)

VALKYRIE COMODO

Activity Details

PACKER

The binary likely contains encrypted or compressed data. Show sources

VALKYRIE COMODO

Behavior Graph

07:15:11 **07:15:11** **07:15:11**

PID 2860

07:15:11	Create Process	The malicious file created a child process as 519c595797b293f4977654c8c61ae80dc735b703.exe **(PPID 1640)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
C:\Users\user\AppData\Local\Temp\plugins*.dll
C:\Users\user\AppData\Local\Temp\clt.html
\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\SYSTEM\ControlSet001\Control\Nls\Locale\00000409
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\Language Groups\1
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
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\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Tahoma
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

uxtheme.dll.ThemeInitApiHook
user32.dll.IsProcessDPIAware
dwmapi.dll.DwmIsCompositionEnabled
comctl32.dll.RegisterClassNameW
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
uxtheme.dll.EnableThemeDialogTexture
uxtheme.dll.OpenThemeData
uxtheme.dll.GetThemeBool
uxtheme.dll.IsThemePartDefined
uxtheme.dll.GetThemePartSize
uxtheme.dll.GetThemeFont
uxtheme.dll.GetThemeColor
imm32.dll.ImmIsIME
uxtheme.dll.CloseThemeData
uxtheme.dll.GetThemeTextExtent
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
uxtheme.dll.GetThemeMargins
gdi32.dll.GdiIsMetaPrintDC
ole32.dll.CoInitializeEx
ole32.dll.CoUninitialize
cryptbase.dll.SystemFunction036
ole32.dll.CoRegisterInitializeSpy
ole32.dll.CoRevokeInitializeSpy
uxtheme.dll.GetThemeInt
uxtheme.dll.DrawThemeBackground
uxtheme.dll.BufferedPaintInit
uxtheme.dll.BufferedPaintRenderAnimation
uxtheme.dll.BeginBufferedAnimation
uxtheme.dll.IsThemeBackgroundPartiallyTransparent
uxtheme.dll.DrawThemeParentBackground
uxtheme.dll.GetThemeBackgroundContentRect
uxtheme.dll.DrawThemeText
uxtheme.dll.EndBufferedAnimation
uxtheme.dll.DrawThemeTextEx
uxtheme.dll.BeginBufferedPaint
uxtheme.dll.EndBufferedPaint

REGISTRY KEYS

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_CURRENT_USER
HKEY_CURRENT_USER\Control Panel\Desktop
HKEY_CURRENT_USER\Control Panel\Desktop\SmoothScroll

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\EnableBalloonTips
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewAlphaSelect
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ListviewShadow
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\AccListViewV6
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\UseDoubleClickTimer
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\FontSubstitutes
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\FontSubstitutes\Segoe UI
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 NT\CurrentVersion\FontSubstitutes\Tahoma
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback\Tahoma
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\CTF\Compatibility\519c595797b293f4977654c8c61ae80dc735b703.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\CTF\KnownClasses

READ FILES

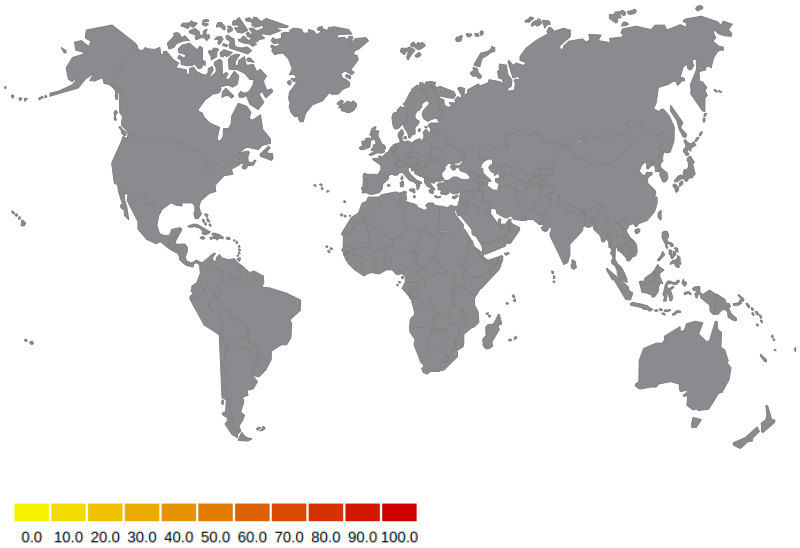
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\Fonts\staticcache.dat
\Device\KsecDD

MUTEXES

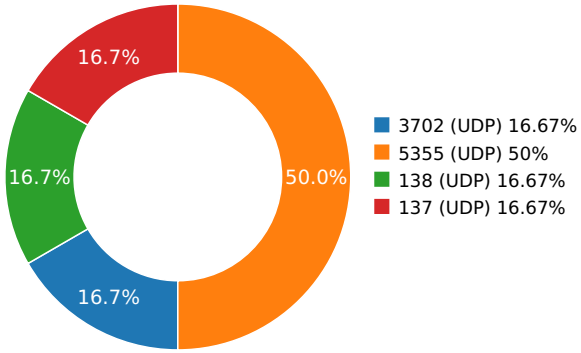
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1

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
6.54193305969	Sandbox	224.0.0.252	5355
6.67040896416	Sandbox	192.168.56.255	137
6.75792002678	Sandbox	224.0.0.252	5355
6.83702993393	Sandbox	239.255.255.250	3702
9.3242828846	Sandbox	224.0.0.252	5355
9.68088293076	Sandbox	192.168.56.255	138

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\Clt.Html	**Type :** HTML document, ASCII text, with very long lines, with no line terminators **MD5 :** fb4eb6db02b2c721636443938c357a17 **SHA-1 :** 26c17321739841956bc8ead5681c26f12440e615 **SHA-256 :** 945d2dd127891847e8ff0aa9910d3705340ae0f5 **SHA-512 :** faadd70438110145f37a0abd1736d232692758f5 **Size :** 0.954 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	clt.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	519c595797b293f4977654c8c61ae80dc735b703
MD5:	db74dd8cfe19e770a65baade28b7bdf1
First Seen Date:	2015-09-06 13:39:24.660000 (7 years ago)
Number Of Clients Seen:	44
Last Analysis Date:	2022-08-01 11:45:43.118083 (23 days ago)
Human Expert Analysis Date:	2016-01-27 13:21:56.414497 (7 years 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	[]
Compilation Time Stamp	0x491DBD88 [Fri Nov 14 18:03:52 2008 UTC]
Entry Point	0x402080 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	118784
Ssdeep	
Sha256	63a82355d257d0a9c5538638b44f764c4f40b3ca9f9a7023f0886d9afa93df2d
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x1624	0x2000	4.60646115072	c27d5c9a3ff0b23da089b60c75bf126b
.rdata	0x3000	0x128e	0x2000	3.81273468807	8a3a71cdd41550bb08d257e6d776a40a
.data	0x5000	0xbc	0x1000	0.0922169849735	6f00ee2587175f18387366f923c8b598
.rsrc	0x6000	0x16880	0x17000	7.31786873968	2f8119ba60a8bc551a4469c7a171e1e8

PE Resources

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_BITMAP', u'offset': 34016, u'sha256': u'0d7ca4bc8e8b915099af7c2c146672e920f03f1e4a6c19194080a2302a1677a1', u'type': u'data', u'size': 82842}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_ICON', u'offset': 26280, u'sha256': u'4721862acb904899dd09c978cd1ca2c10b2bca46a66240cbf33bc83452053ced', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_ICON', u'offset': 27408, u'sha256': u'f2ffeab20c04ec67eb965c5f977d71ba664bffef156a2be431254552a242a771', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_ICON', u'offset': 31712, u'sha256': u'fa0e2b1cf4380f14b026c86a5c4f5b50e5d5bfa1d5f158be9f41b87761f97009', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_ICON', u'offset': 32864, u'sha256': u'67730b7372395a2a71b362919e532985a2ba5f0a672e56ca8e83f1e30a652fd2', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_DIALOG', u'offset': 25200, u'sha256': u'40e7f303bf826d373857069b4d1ea977b77fe842887c34d92df43035a84829d2', u'type': u'data', u'size': 386}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_GROUP_ICON', u'offset': 31672, u'sha256': u'b1a9ff73f6a9d486c67f409a629924792ca40aa8966d45e48239863f63629fd0', u'type': u'MS Windows icon resource - 2 icons, 16x16', u'size': 34}

{u'lang': u'LANG_RUSSIAN', u'name': u'RT_GROUP_ICON', u'offset': 32840, u'sha256':

u'5caad09ee058fd7d52f197cd92a152814a2fa8858cd197d2923002d12098aee5', u'type': u'MS Windows icon resource - 1 icon, 16x16', u'size': 20}

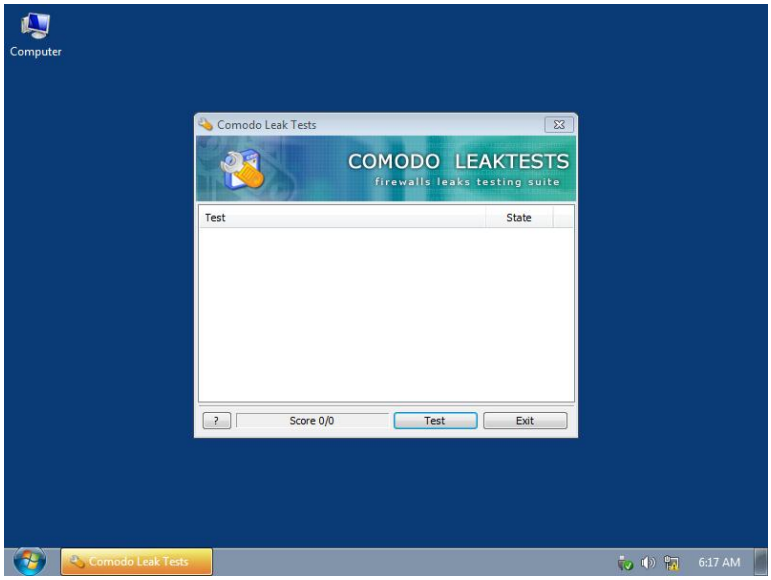
{u'lang': u'LANG_RUSSIAN', u'name': u'RT_GROUP_ICON', u'offset': 33992, u'sha256': u'd6659139f55adad2497df8d1a11fcd68324a00ccdadbc133ddd49fb79e9ccc1c', u'type': u'MS Windows icon resource - 1 icon, 16x16', u'size': 20}

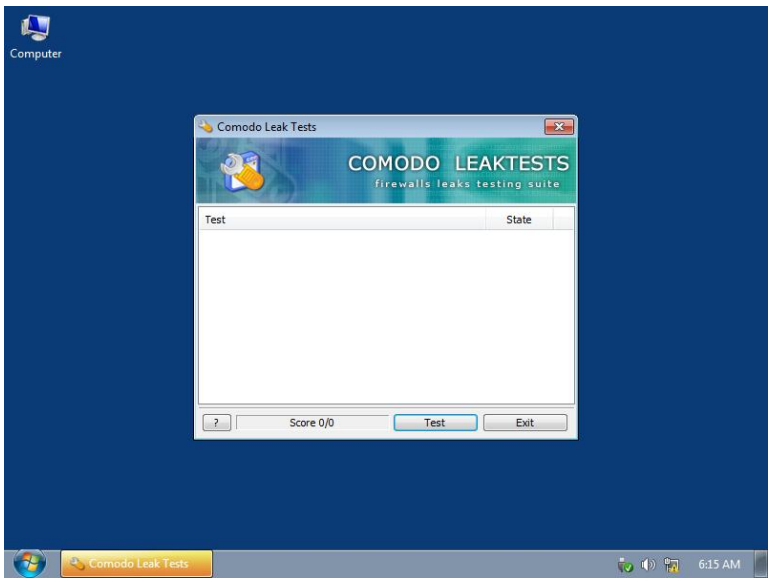
{u'lang': u'LANG_RUSSIAN', u'name': u'RT_MANIFEST', u'offset': 25592, u'sha256': u'55158892136111b1042e7779551a84e31294021ac57b66d8bb9465debb10d7a5', u'type': u'XML 1.0 document, ASCII text, with CRLF line terminators', u'size': 685}

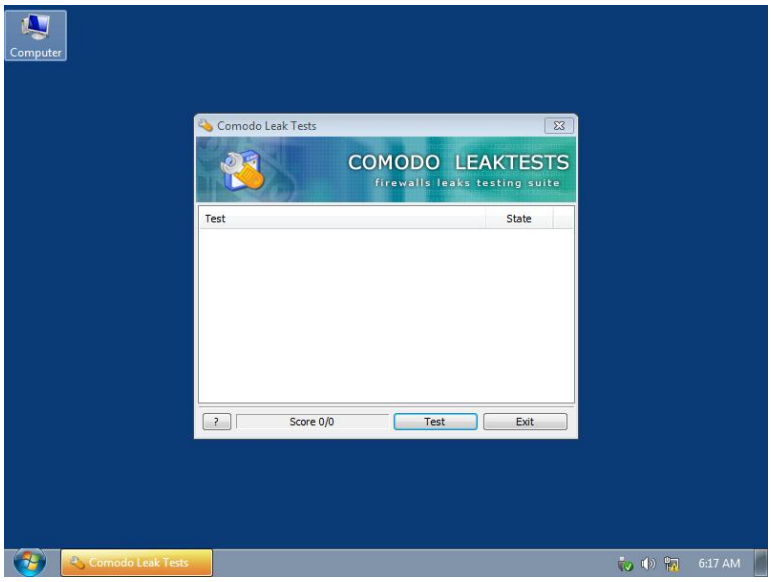
CERTIFICATE VALIDATION

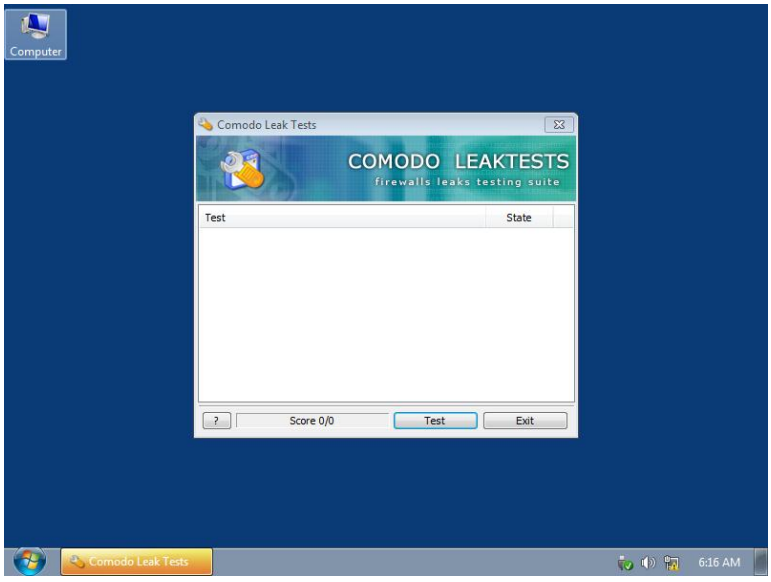
- Certificate Validation is not Applicable ?

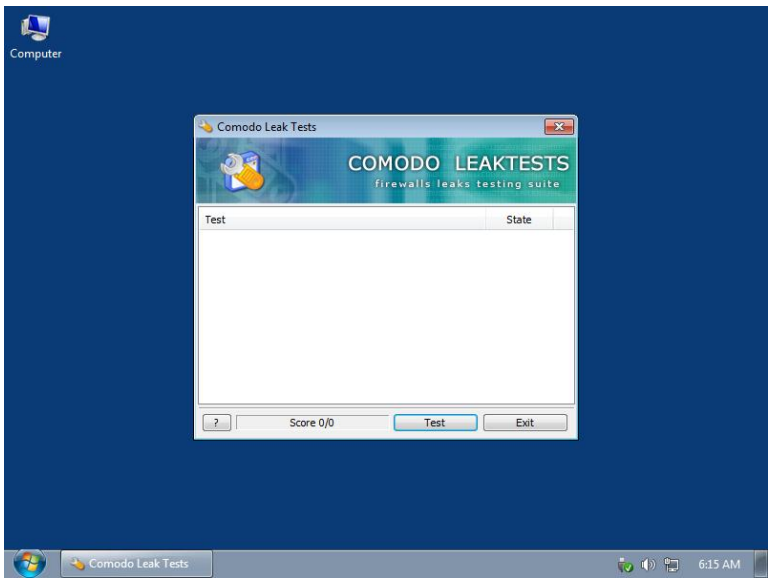
SCREENSHOTS

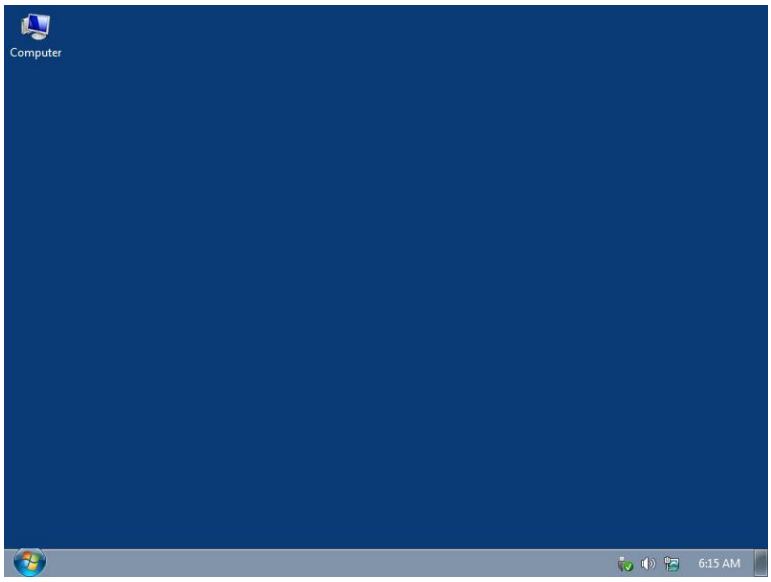


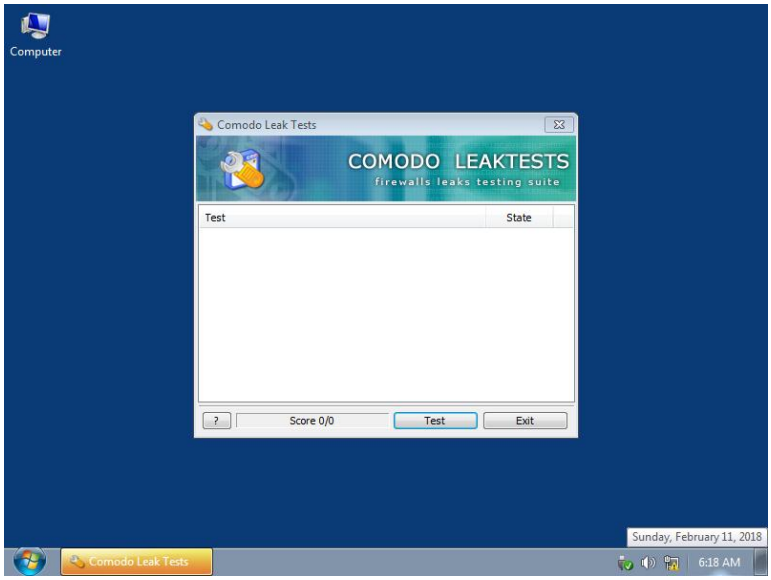


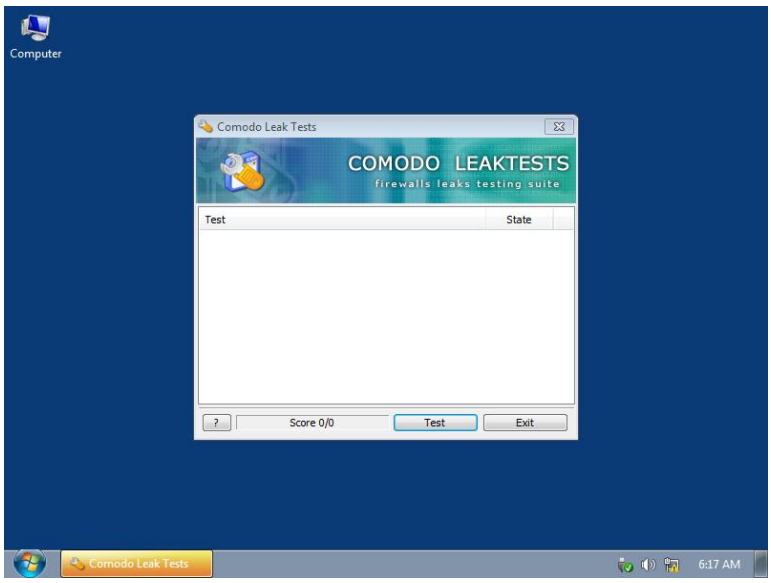

Computer
Comodo Leak Tests
COMODO LEAKTESTS
firewalls leaks testing suite
Test
State
?
Score 0/0
Test
Exit
Comodo Leak Tests
6:17 AM

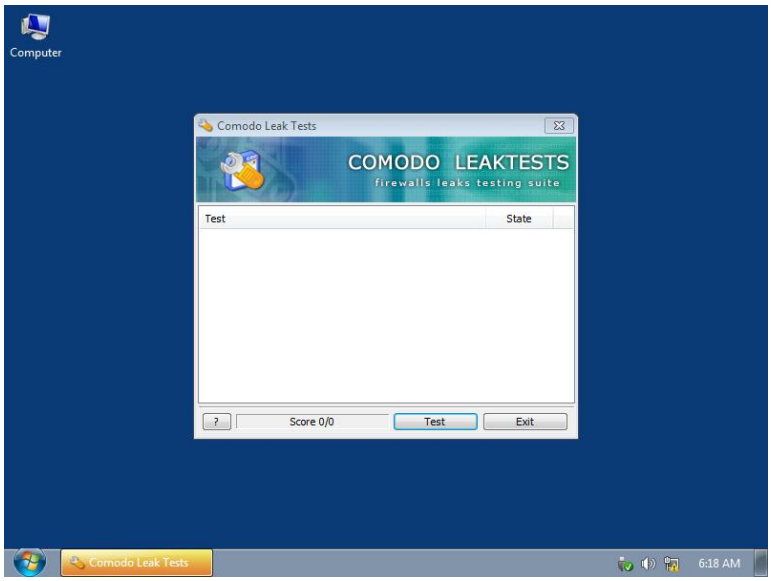

Computer
Comodo Leak Tests
COMODO LEAKTESTS
firewalls leaks testing suite
Test
State
?
Score 0/0
Test
Exit
Comodo Leak Tests
6:16 AM

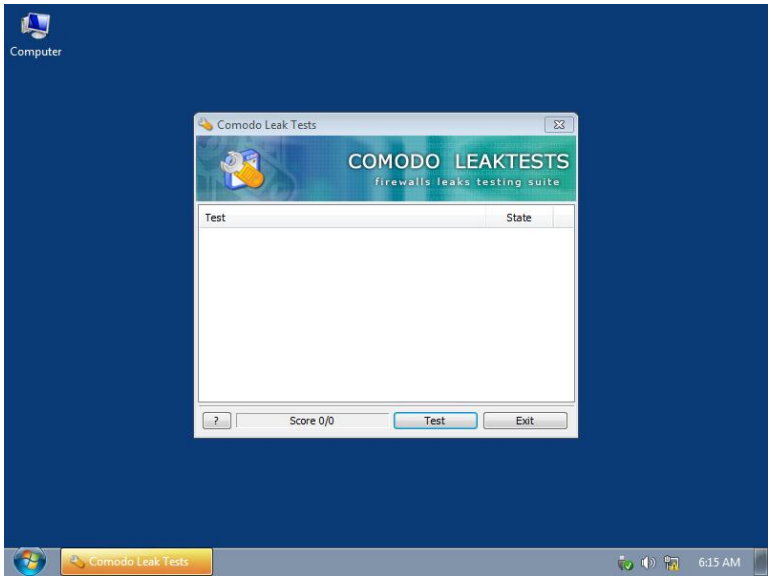

Computer
Comodo Leak Tests
COMODO LEAKTESTS
firewalls leaks testing suite
Test
State
?
Score 0/0
Test
Exit
Comodo Leak Tests
6:15 AM


Computer
6:15 AM


Computer
Comodo Leak Tests
COMODO LEAKTESTS
firewalls leaks testing suite
Test
State
?
Score 0/0
Test
Exit
Sunday, February 11, 2018
Comodo Leak Tests
6:18 AM


Computer
Comodo Leak Tests
COMODO LEAKTESTS
firewalls leaks testing suite
Test
State
?
Score 0/0
Test
Exit
Comodo Leak Tests
6:17 AM


Computer
Comodo Leak Tests
COMODO LEAKTESTS
firewalls leaks testing suite
Test
State
?
Score 0/0
Test
Exit
Comodo Leak Tests
6:18 AM


Computer
Comodo Leak Tests
COMODO LEAKTESTS
firewalls leaks testing suite
Test
State
?
Score 0/0
Test
Exit
Comodo Leak Tests
6:15 AM