VALKYRIE COMODO

Summary

File Name: ascsetup.exe

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

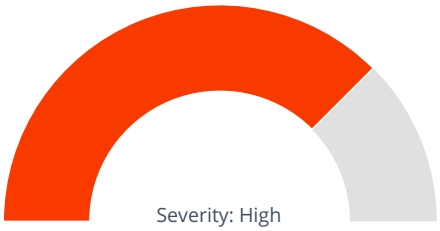
SHA1: 09a79205a2666900daf1469068460007c1b2de63

MD5: 51abd9368b1ff9d36d3d7f4075855f6e

MALWARE

Valkyrie Final Verdict

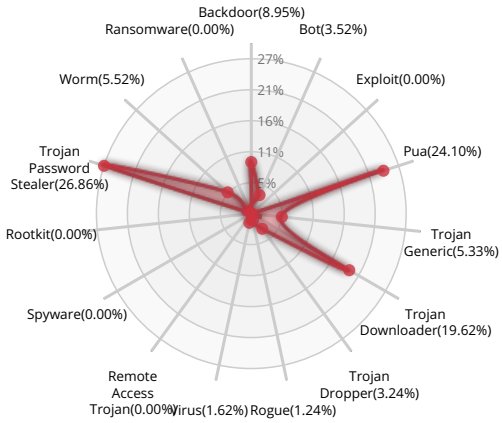
DETECTION SECTION



Severity: High

Verdict: Malware

CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION

ACTIVITY OVERVIEW

Networking 2 (100.00%)

VALKYRIE COMODO

Activity Details

NETWORKING

HTTP traffic contains suspicious features which may be indicative of malware related traffic — Show sources

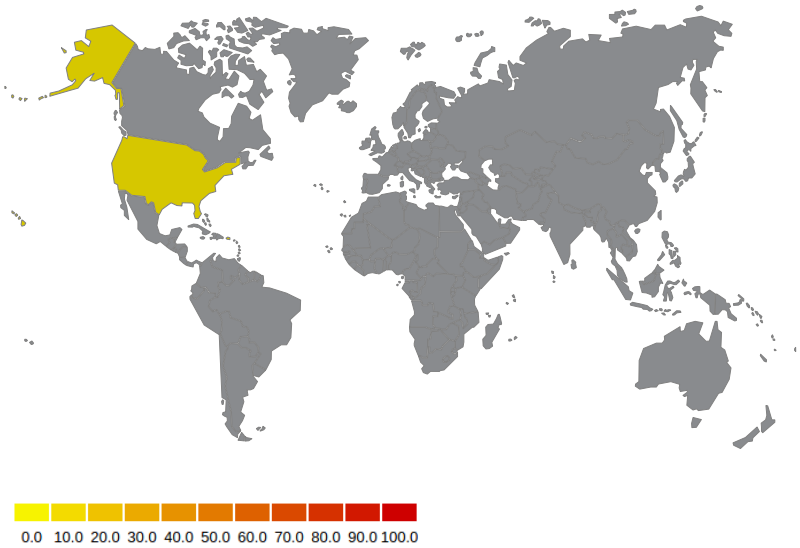
Performs some HTTP requests — Show sources

Behavior Graph

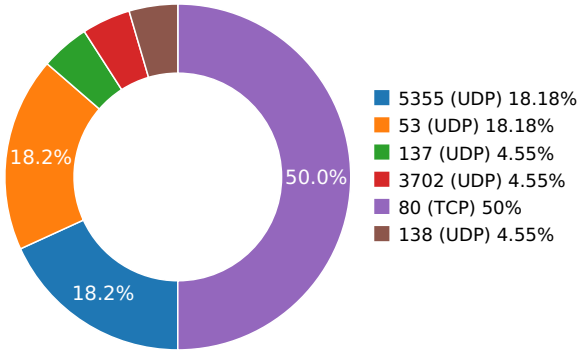
Behavior Summary

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	69.164.0.128	United States	22822	Limelight Networks, Inc.	Malware Process
	208.111.178.129		22822	Limelight Networks, Inc.	Malware Process
	216.245.208.194		46475	Limestone Networks, Inc.	Malware Process
	208.111.178.129		22822	Limelight Networks, Inc.	Malware Process
	184.173.21.164		36351	SoftLayer Technologies Inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
cc.ppacti.com	80	GET	1.1		1	10.2542359829
Path: /productprice.svc/getcountrycode **URI:** http://cc.ppacti.com/productprice.svc/getcountrycode						
www.ppacti.com	80	GET	1.1		1	10.494353056
Path: /getip/ **URI:** http://www.ppacti.com/getip/						
trkr.ppacti.com	80	GET	1.1		1	10.7968211174
Path: /ipfiles/192_241_99_194.txt **URI:** http://trkr.ppacti.com/ipfiles/192_241_99_194.txt						
www.ppacti.com	80	GET	1.1		1	14.7959201336
Path: /install/asc?utm_source=cccleanersite&utm_campaign=cccleanersite&utm_medium=cccleanersite&utm_pubid=&pxl=cccleanersite&x-context=&x-at=&x-uid=6656332131250686 50&sysname=&syslogo=&x-dm=aHR0cDovL3d3dy5hZHZhbmNlcGN0b29scy5uZXQv&x-ccode=us&x-count=0&x-ip=192_241_99_194&x-fetch=0 **URI:** http://www.ppacti.com/install/asc?utm_source=cccleanersite&utm_campaign=cccleanersite&utm_medium=cccleanersite&utm_pubid=&pxl=cccleanersite&x-context=&x-at=&x-uid=6656332131250686 50&sysname=&syslogo=&x-dm=aHR0cDovL3d3dy5hZHZhbmNlcGN0b29scy5uZXQv&x-ccode=us&x-count=0&x-ip=192_241_99_194&x-fetch=0						
www.ppacti.com	80	GET	1.1		1	14.8511090279
Path: /install/asc/?utm_source=cccleanersite&utm_campaign=cccleanersite&utm_medium=cccleanersite&utm_pubid=&pxl=cccleanersite&x-context=&x-at=&x-uid=6656332131250686 50&sysname=&syslogo=&x-dm=aHR0cDovL3d3dy5hZHZhbmNlcGN0b29scy5uZXQv&x-ccode=us&x-count=0&x-ip=192_241_99_194&x-fetch=0 **URI:** http://www.ppacti.com/install/asc/?utm_source=cccleanersite&utm_campaign=cccleanersite&utm_medium=cccleanersite&utm_pubid=&pxl=cccleanersite&x-context=&x-at=&x-uid=6656332131250686 50&sysname=&syslogo=&x-dm=aHR0cDovL3d3dy5hZHZhbmNlcGN0b29scy5uZXQv&x-ccode=us&x-count=0&x-ip=192_241_99_194&x-fetch=0						
cdn.advancepctools.net	80	GET	1.1		1	20.6443450451
Path: /asc/asc_upgrades/upgrade_en_us.xml **URI:** http://cdn.advancepctools.net/asc/asc_upgrades/upgrade_en_us.xml						

DNS QUERIES

Request	Type
cc.ppacti.com	A
Answers - 216.245.208.194 (A)	
www.ppacti.com	A
Answers - 184.173.21.164 (A) - ppacti.com (CNAME)	
trkr.ppacti.com	A
Answers - 69.164.0.0 (A) - 69.164.0.128 (A) - pcvark.vo.llnwd.net (CNAME)	
cdn.advancepctools.net	A
Answers - pcvarkr.vo.llnwd.net (CNAME)	

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
10.2542359829	Sandbox	216.245.208.194	80
10.494353056	Sandbox	184.173.21.164	80
10.7968211174	Sandbox	69.164.0.128	80
14.7959201336	Sandbox	184.173.21.164	80
20.6443450451	Sandbox	69.164.0.128	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.08082604408	Sandbox	224.0.0.252	5355
3.121778965	Sandbox	224.0.0.252	5355
3.12798905373	Sandbox	192.168.56.255	137
3.12819600105	Sandbox	239.255.255.250	3702
5.67286515236	Sandbox	224.0.0.252	5355
6.98080801964	Sandbox	192.168.56.255	138
10.1757991314	Sandbox	8.8.4.4	53
10.385833025	Sandbox	8.8.4.4	53
10.7123270035	Sandbox	8.8.4.4	53
12.1802690029	Sandbox	224.0.0.252	5355
20.5891411304	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	ascsetup.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	09a79205a2666900daf1469068460007c1b2de63
MD5:	51abd9368b1ff9d36d3d7f4075855f6e
First Seen Date:	2017-10-19 08:13:37.709288 (about a year ago)
Number Of Clients Seen:	4
Last Analysis Date:	2017-10-19 08:13:37.709288 (about a year ago)
Human Expert Analysis Date:	2017-11-28 15:43:45.675133 (about a year ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
File Type Enum	6
Number Of Sections	8
Compilation Time Stamp	0x5698AC5A [Fri Jan 15 08:22:50 2016 UTC]
LegalCopyright	
FileVersion	1.0.0.2509
CompanyName	
Comments	This installation was built with Inno Setup.
ProductName	Advance -System Care
ProductVersion	1.0.0.2509
FileDescription	Advance -System Care Setup
Translation	0x0000 0x04b0
Entry Point	0x4113bc (.itext)
Machine Type	Intel 386 or later - 32Bit
File Size	5151312
Sha256	ef119cb084ee0d8a993352f6c1c2e6983b97fb0e40e42ad6cd0b316baf1bc972
Mime Type	application/x-dosexec

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0xf134	0xf200	6.39169445915	1a600bbd86f701d3e6b2978b57906082
.itext	0x11000	0xb44	0xc00	5.7430519764	0b6f227afa44fd825f60bccacb9073bf
.data	0x12000	0xc88	0xe00	2.24753305436	da9cb156b6104ba552cb70804b8a50a3
.bss	0x13000	0x56b8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.idata	0x19000	0xdd0	0xe00	4.97188203377	93d91a2b90e60bd758fc0c4908856ae1
.tls	0x1a000	0x8	0x0	0.0	d41d8cd98f00b204e9800998ecf8427e
.rdata	0x1b000	0x18	0x200	0.20448815744	3dffc444ccc131c9dcee18db49ee6403
.rsrc	0x1c000	0x179c8	0x17a00	5.11453460613	3d5fc736680c3cef38f81095ef17923d

PE Imports

- oleaut32.dll
  - SysFreeString
  - SysReAllocStringLen
  - SysAllocStringLen
- advapi32.dll

    - RegQueryValueExW
    - RegOpenKeyExW
    - RegCloseKey
- user32.dll
    - GetKeyboardType
    - LoadStringW
    - MessageBoxA
    - CharNextW
- kernel32.dll
    - GetACP
    - Sleep
    - VirtualFree
    - VirtualAlloc
    - GetSystemInfo
    - GetTickCount
    - QueryPerformanceCounter
    - GetVersion
    - GetCurrentThreadId
    - VirtualQuery
    - WideCharToMultiByte
    - MultiByteToWideChar
    - lstrlenW
    - lstrcpynW
    - LoadLibraryExW
    - GetThreadLocale
    - GetStartupInfoA
    - GetProcAddress
    - GetModuleHandleW
    - GetModuleFileNameW
    - GetLocaleInfoW
    - GetCommandLineW
    - FreeLibrary
    - FindFirstFileW
    - FindClose
    - ExitProcess
    - WriteFile
    - UnhandledExceptionFilter
    - RtlUnwind
    - RaiseException
    - GetStdHandle
    - CloseHandle
- kernel32.dll
    - TlsSetValue
    - TlsGetValue
    - LocalAlloc
    - GetModuleHandleW
- user32.dll
    - CreateWindowExW
    - TranslateMessage
    - SetWindowLongW
    - PeekMessageW
    - MsgWaitForMultipleObjects
    - MessageBoxW
    - LoadStringW
    - GetSystemMetrics
    - ExitWindowsEx
    - DispatchMessageW
    - DestroyWindow
    - CharUpperBuffW
    - CallWindowProcW
- kernel32.dll
    - WriteFile
    - WideCharToMultiByte
    - WaitForSingleObject
    - VirtualQuery
    - VirtualProtect
    - VirtualFree
    - VirtualAlloc
    - SizeofResource
    - SignalObjectAndWait
    - SetLastError
    - SetFilePointer
    - SetEvent
    - SetErrorMode
    - SetEndOfFile

    - ResetEvent
    - RemoveDirectoryW
    - ReadFile
    - MultiByteToWideChar
    - LockResource
    - LoadResource
    - LoadLibraryW
    - GetWindowsDirectoryW
    - GetVersionExW
    - GetUserDefaultLangID
    - GetThreadLocale
    - GetSystemInfo
    - GetStdHandle
    - GetProcAddress
    - GetModuleHandleW
    - GetModuleFileNameW
    - GetLocaleInfoW
    - GetLastError
    - GetFullPathNameW
    - GetFileSize
    - GetFileAttributesW
    - GetExitCodeProcess
    - GetEnvironmentVariableW
    - GetDiskFreeSpaceW
    - GetCurrentProcess
    - GetCommandLineW
    - GetCPInfo
    - InterlockedExchange
    - InterlockedCompareExchange
    - FreeLibrary
    - FormatMessageW
    - FindResourceW
    - EnumCalendarInfoW
    - DeleteFileW
    - CreateProcessW
    - CreateFileW
    - CreateEventW
    - CreateDirectoryW
    - CloseHandle
- advapi32.dll
    - RegQueryValueExW
    - RegOpenKeyExW
    - RegCloseKey
    - OpenProcessToken
    - LookupPrivilegeValueW
- comctl32.dll
    - InitCommonControls
- kernel32.dll
    - Sleep
- advapi32.dll
    - AdjustTokenPrivileges

PE Resources

RT_ICON
RT_STRING
RT_RCDATA
RT_GROUP_ICON
RT_VERSION
RT_MANIFEST

CERTIFICATE VALIDATION

- Success ✔

[+] PC-Speedup-Tools-Inc	
Status	NoError ✔
Start Date	2017-09-20 00:00:00+00:00
End Date	2018-09-07 23:59:59+00:00
Sha256	9e94994c89801210744f74b1c46e265c8a4a0aaaa92e1f0df68f057ba9cff383
Serial	00E97D4FB2265E0FD6FB39FC9C5E9CE3F4
Subject Key Identifier	88 f7 57 00 1d f4 80 99 3a a3 18 30 ba 3d 08 83 95 06 b4 4e
Issuer Name	COMODO RSA Code Signing CA
Issuer Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Crl link	http://crl.comodoca.com/COMODORSACodeSigningCA.crl
Key Usage	Digital Signature (80)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

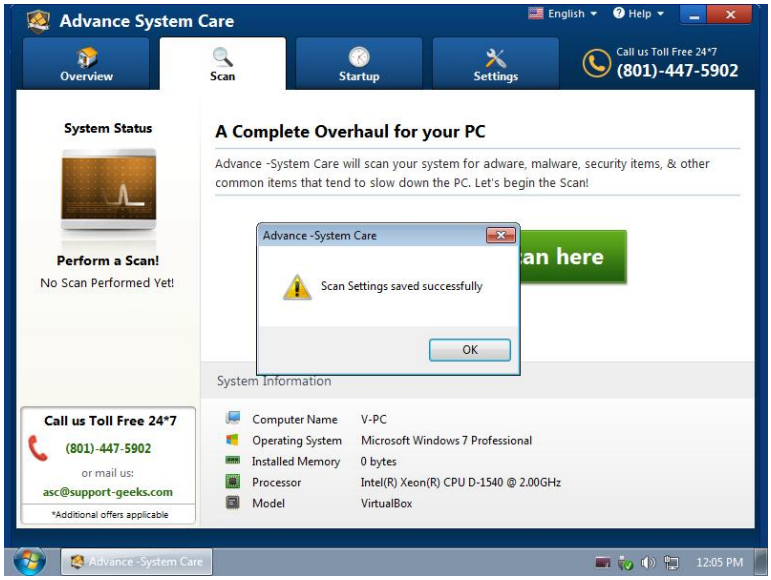
[+] COMODO RSA Code Signing CA	
Status	NoError ✔
Start Date	2013-05-09 00:00:00+00:00
End Date	2028-05-08 23:59:59+00:00
Sha256	be4b37864cefc39611d4b6a1de110074e5f282de90016aa5d36849ab452eab2c
Serial	2E7C87CC0E934A52FE94FD1CB7CD34AF
Subject Key Identifier	29 91 60 ff 8a 4d fa eb f9 a6 6a b8 cf f9 e6 4b bd 49 ce 12
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Crl link	http://crl.comodoca.com/COMODORSACertificationAuthority.crl
Key Usage	Digital Signature,Certificate Signing,Off-line CRL Signing,CRL Signing (86)
Extended Usage	Code Signing (1.3.6.1.5.5.7.3.3)

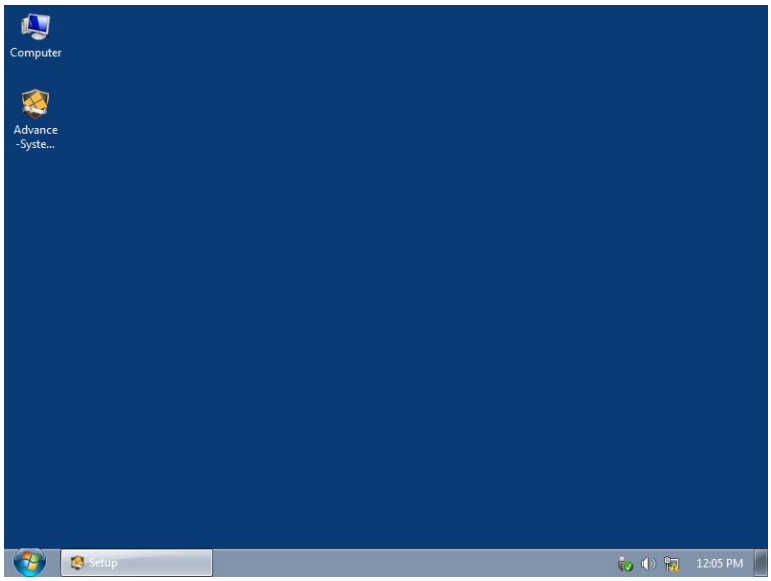
[+] COMODO RSA Certification Authority	
Status	NoError ✔
Start Date	2010-01-19 00:00:00+00:00
End Date	2038-01-18 23:59:59+00:00
Sha256	f1bc8293a80c7d1bb2fd1d6e9b714b06e6b66686ca9b26a76d91e06e2934fa83
Serial	4CAAF9CADB636FE01FF74ED85B03869D
Subject Key Identifier	bb af 7e 02 3d fa a6 f1 3c 84 8e ad ee 38 98 ec d9 32 32 d4
Issuer Name	COMODO RSA Certification Authority
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

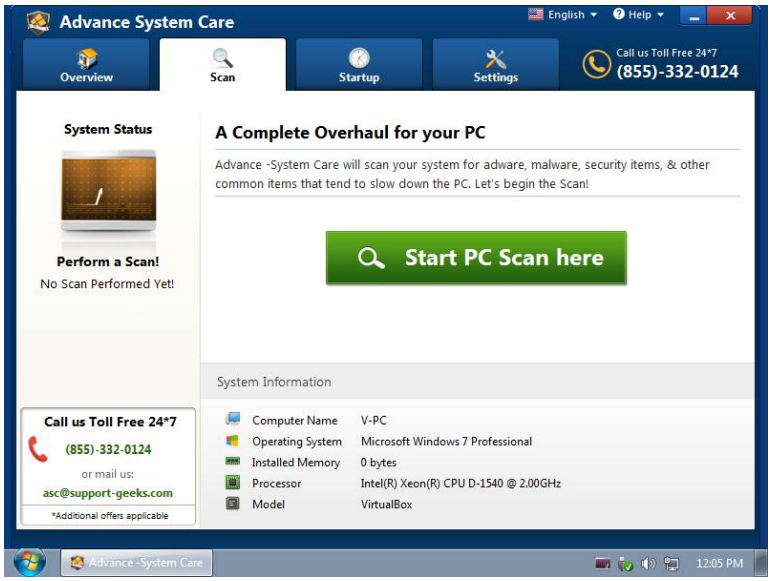
[+] GlobalSign Timestamping CA - G2	
Status	NoError ✔
Start Date	2011-04-13 10:00:00+00:00
End Date	2028-01-28 12:00:00+00:00
Sha256	0f870989c6b1f8082f91361833e8a61864a760c50594398911ffe34531cd1065
Serial	0400000000012F4EE152D7
Subject Key Identifier	46 d8 3e ff dc e3 be ff 83 e6 f4 85 9b b0 dd 6a d6 14 a9 c1
Issuer Name	GlobalSign Root CA
Issuer Key Identifier	60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b
Crl link	http://crl.globalsign.net/root.crl
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

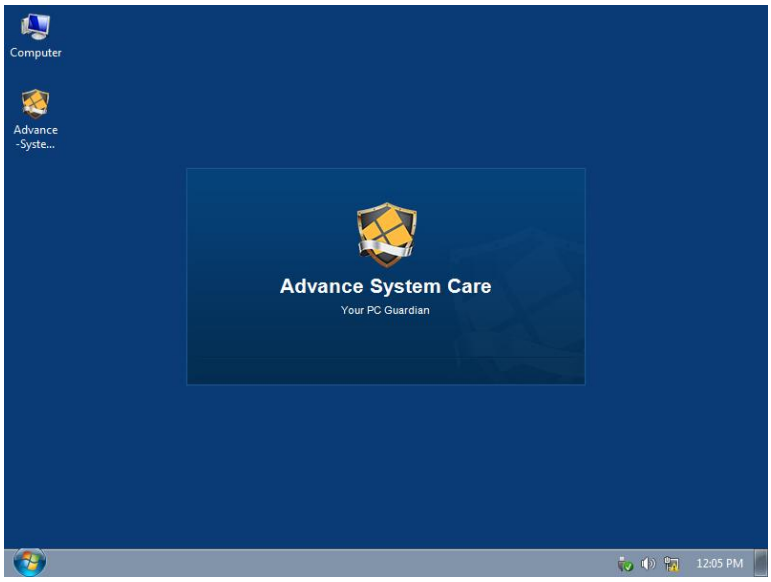
[+] GlobalSign Root CA	
Status	NoError ✔
Start Date	1998-09-01 12:00:00+00:00
End Date	2028-01-28 12:00:00+00:00
Sha256	8890262a3cd37c0b6c37c0239b9533f33244fb4ec82b6d846f6bd379ed2184b7
Serial	040000000001154B5AC394
Subject Key Identifier	60 7b 66 1a 45 0d 97 ca 89 50 2f 7d 04 cd 34 a8 ff fc fd 4b
Issuer Name	GlobalSign Root CA
Issuer Key Identifier	undefined
Crl link	undefined
Key Usage	Certificate Signing,Off-line CRL Signing,CRL Signing (06)
Extended Usage	undefined

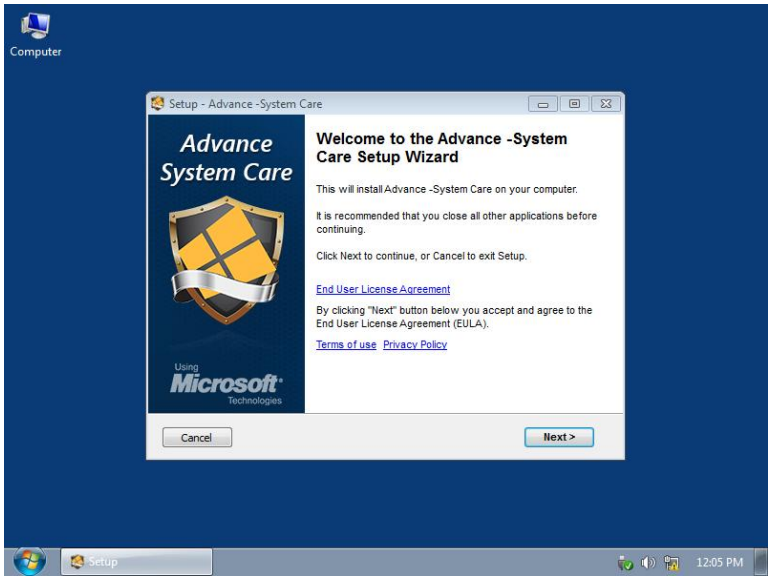
SCREENSHOTS

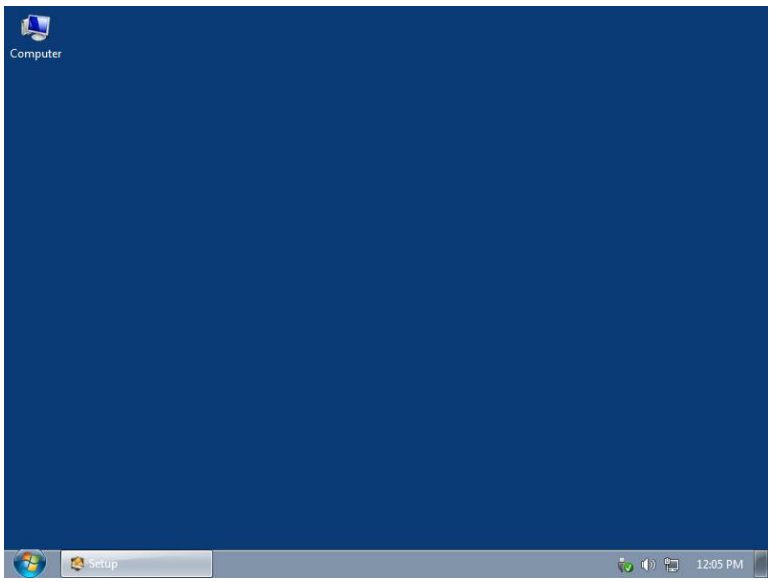

Advance System Care
English
Help
Overview
Scan
Startup
Settings
Call us Toll Free 24*7
(801)-447-5902
System Status
Perform a Scan!
No Scan Performed Yet!
A Complete Overhaul for your PC
Advance -System Care will scan your system for adware, malware, security items, & other common items that tend to slow down the PC. Let's begin the Scan!
Advance -System Care
Scan Settings saved successfully
OK
an here
System Information
Computer Name V-PC
Operating System Microsoft Windows 7 Professional
Installed Memory 0 bytes
Processor Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
Model VirtualBox
Call us Toll Free 24*7
(801)-447-5902
or mail us:
asc@support-geeks.com
*Additional offers applicable
Advance -System Care
12:05 PM

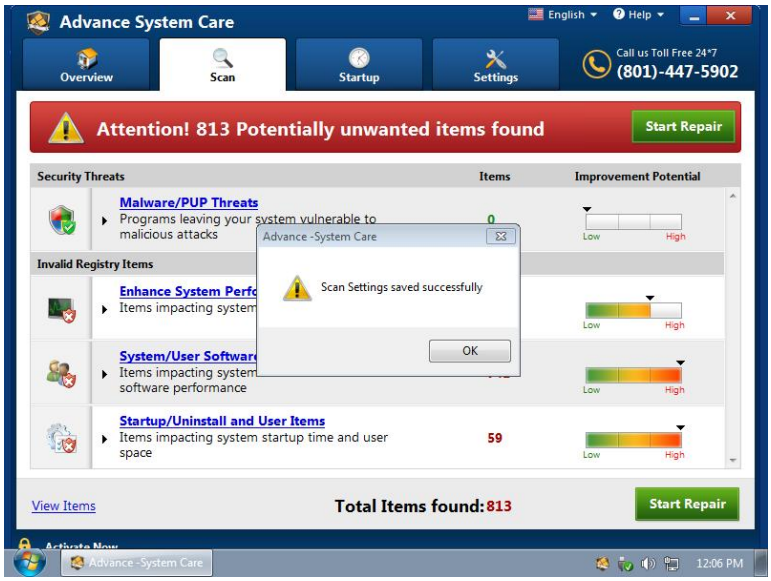

Computer
Advance -Syste...
Setup
12:05 PM

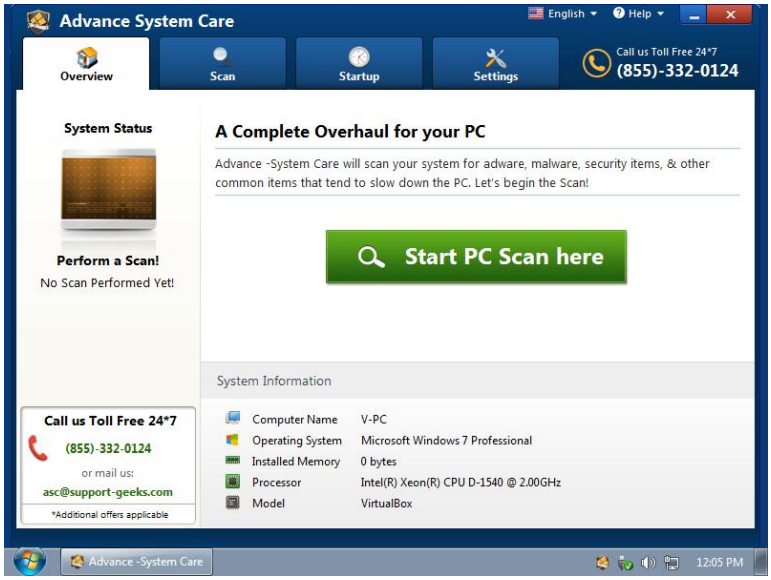

Advance System Care
English
Help
Overview
Scan
Startup
Settings
Call us Toll Free 24*7
(855)-332-0124
System Status
Perform a Scan!
No Scan Performed Yet!
A Complete Overhaul for your PC
Advance -System Care will scan your system for adware, malware, security items, & other common items that tend to slow down the PC. Let's begin the Scan!
Start PC Scan here
System Information
Computer Name V-PC
Operating System Microsoft Windows 7 Professional
Installed Memory 0 bytes
Processor Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
Model VirtualBox
Call us Toll Free 24*7
(855)-332-0124
or mail us:
asc@support-geeks.com
*Additional offers applicable
Advance -System Care
12:05 PM


Computer
Advance -Syste...
Advance System Care
Your PC Guardian
12:05 PM


Computer
Setup - Advance -System Care
Advance System Care
Welcome to the Advance -System Care Setup Wizard
This will install Advance -System Care on your computer.
It is recommended that you close all other applications before continuing.
Click Next to continue, or Cancel to exit Setup.
End User License Agreement
By clicking "Next" button below you accept and agree to the End User License Agreement (EULA).
Terms of use Privacy Policy
Using Microsoft Technologies
Cancel
Next >
Setup
12:05 PM


Computer
Setup
12:05 PM


Advance System Care
English
Help
Overview
Scan
Startup
Settings
Call us Toll Free 24*7
(801)-447-5902
Attention! 813 Potentially unwanted items found
Start Repair
Security Threats
Items
Improvement Potential
Malware/PUP Threats
Programs leaving your system vulnerable to malicious attacks
0
Low
High
Invalid Registry Items
Enhance System Perfo
Items impacting system
System/User Softwar
Items impacting system software performance
Startup/Uninstall and User Items
Items impacting system startup time and user space
59
Advance -System Care
Scan Settings saved successfully
OK
View Items
Total Items found: 813
Start Repair
12:06 PM


Advance System Care
English
Help
Overview
Scan
Startup
Settings
Call us Toll Free 24*7
(855)-332-0124
System Status
Perform a Scan!
No Scan Performed Yet!
A Complete Overhaul for your PC
Advance -System Care will scan your system for adware, malware, security items, & other common items that tend to slow down the PC. Let's begin the Scan!
Start PC Scan here
System Information
Computer Name V-PC
Operating System Microsoft Windows 7 Professional
Installed Memory 0 bytes
Processor Intel(R) Xeon(R) CPU D-1540 @ 2.00GHz
Model VirtualBox
Call us Toll Free 24*7
(855)-332-0124
or mail us:
asc@support-geeks.com
*Additional offers applicable
Advance -System Care
12:05 PM


Computer
Advance -Syste...
12:05 PM