EXHIBIT 87

Andrew Romatz

From: Daniel Doman [dan@direct-revenue.com]
Sent: Monday, April 04, 2005 1:39 PM
To: Joshua Abram
Subject: Fwd: Seems like they found ahexe...

Lets talk about this tomorrow

Begin forwarded message:

> **From:** "Douglas Kee" <doug@direct-revenue.com>
> **Date:** April 4, 2005 1:23:32 PM EDT
> **To:** "'Dan Doman'" <Dan@direct-revenue.com>, "'Raffi Minassian'" <raffi@direct-revenue.com>, "'Chris Dowhan'" <chris@direct-revenue.com>, "'Rodney Hook'" <rod@direct-revenue.com>, "Sathish Dhinakaran" <sathish@direct-revenue.com>, "'Matt Knox'" <matt@direct-revenue.com>
> **Subject: Seems like they found ahexe...**
>
> http://www.webhelper4u.com/
>
> Though I'm not sure why they are associating us with a wallpaper download - http://www.webhelper4u.com/nontransponders/wallpapers4u_4022005.html

WebHelper4U.com

Wallpapers4u.com and Its Massive Popup Adware Installs From pacimedia.com

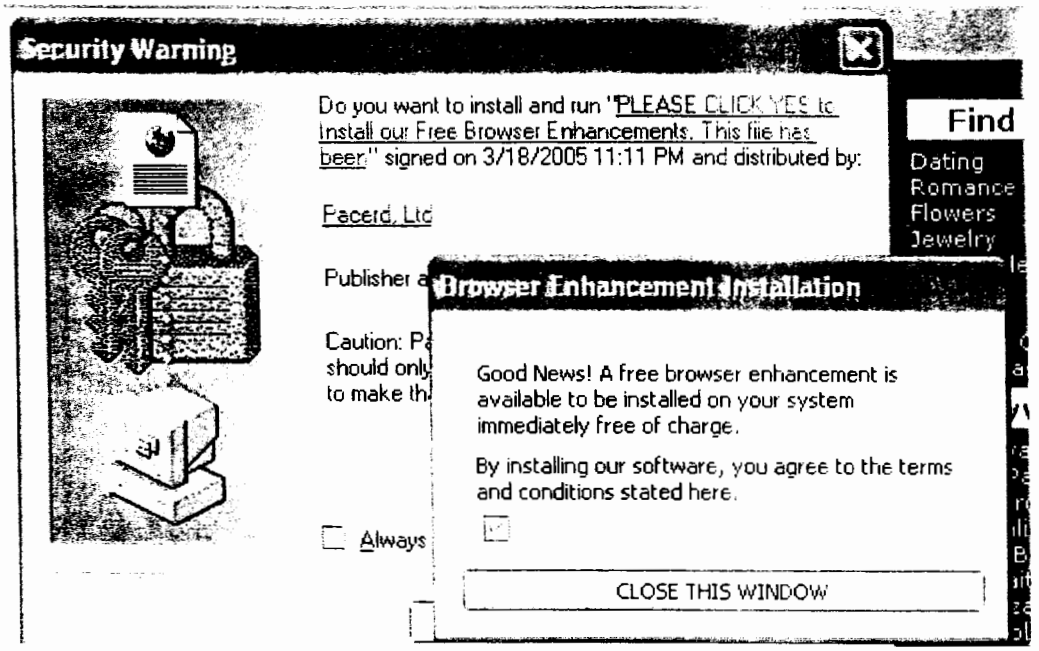
| Home |

Updated: 02 Apr 2005

Direct from the exotic free wallpaper website in India, Walipapers4u.com, if you don't have all the up to date security you can set back and enjoy a **30 plus minute infestation from a supsected CPM Media site: pacimedia.com** if you are not careful with the popup install box's or their windows **media player exploit:** wmplayer.exe.tmp 5kb in size gets into your computer!

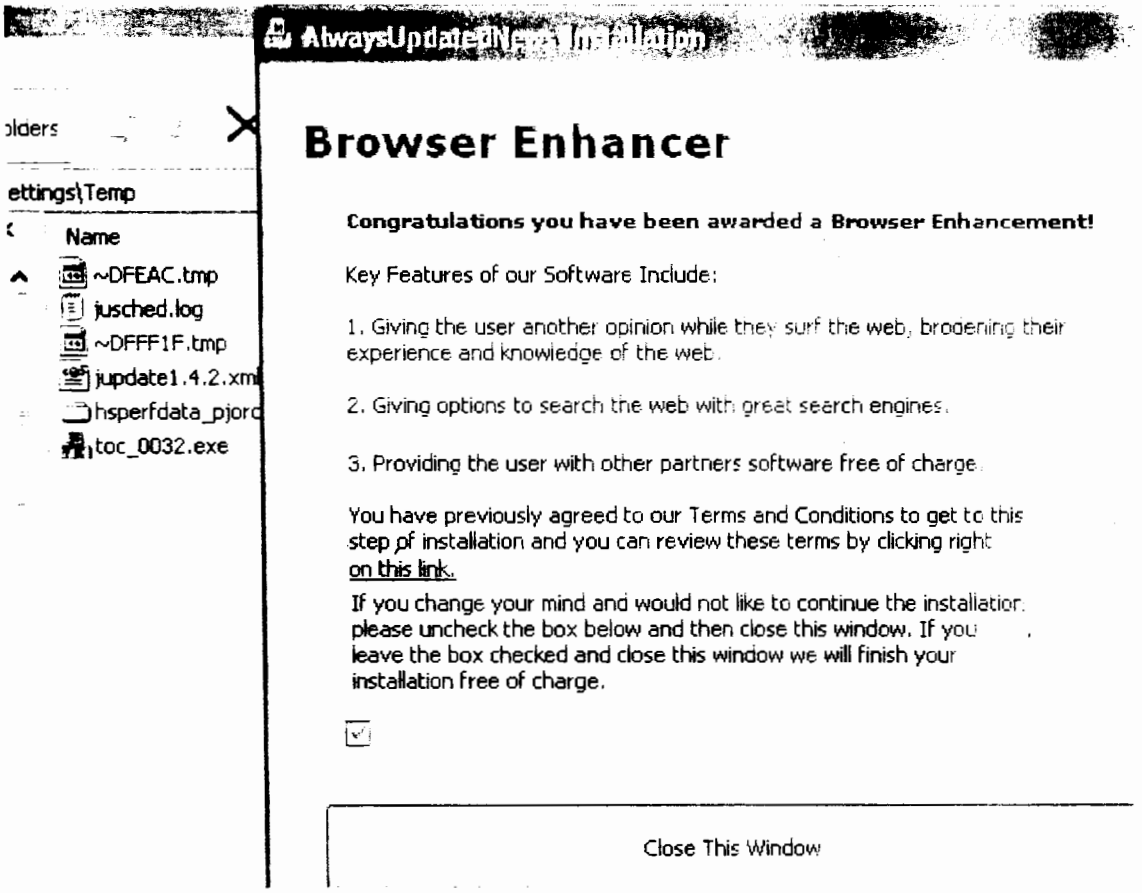
Below you will notice that the first install box is the Security Warning where you can click OK, No, or Cancel or hit the Red X **BUT** as soon as that the Security Warning box appears you also get the Browser Enhancement Installation dialog box which will not allow you to click no.

What the small box does is drop a file into your temp folder named PFT_*.exe where the * is a random number. Each time the box appears another file will also be dropped into the temp folder. **You will also notice that you need to uncheck the Install agreement box** and then click the "**CLOSE THIS WINDOW**" which still if not carefull start the infestation of 3rd party adware.



Ok, say you uncheck the box and click the close this window button. You then get their next "please install me" tacitic.

The second window below is where a toc_*.exe is dropped. This time it states that the user got here because they had previously agreed to the terms. Again you are supposed to uncheck the box and click the close this window.



Now for the best part, after 30 minutes and going over the whole computer to get as many files as possible, below is a list files that came out for the infestations.

C:\ Root and Local Settings Temp folders	**Program Files Folder**
0401[1].exe	**Windows media player Exploit**
1.exe	**windows media player\wmplayer.exe.tmp**
1bfhfp20.dll	
20007.exe	**70kx0a9f\ New ClearSearch Variant**
4241278.dll	70kx0a9f\10189296.txt
a95kfrhe.exe	70kx0a9f\1382770.txt
a95kfrhe.ini	70kx0a9f\14259178.txt
ahexe.exe New Transponder File	70kx0a9f\16192858.txt
aircity.exe	70kx0a9f\19505320.dat
ap2nqrd4.dat	70kx0a9f\20324002.bin
ap9h4qmo.exe	70kx0a9f\21752643.bin
ap9h4qmo.ini	70kx0a9f\26413025.bin
aunps2.dll	70kx0a9f\37353732.exe
authrootseq[1].txt	70kx0a9f\38663579.txt
authrootstl[1].cab	70kx0a9f\42164622.txt
auto_update_uninstall.exe	70kx0a9f\45729992.dat
auto_update_uninstall.log	70kx0a9f\4883754.txt
banner[1]	70kx0a9f\49395445.dat
baur5s9q.dat	70kx0a9f\64529784.bin
bbdi[1].cab	70kx0a9f\65895048.bin

bqrufs5f.dat	70kx0a9f\70151517.bin
bundlelite_westfrontier1001.exe	70kx0a9f\70kx0a9f.dll
cabmxs.exe	70kx0a9f\70kx0a9f.exe
casino-on-net.ico	70kx0a9f\77527253.dat
ceres.dll	70kx0a9f\7xwqsavz.dll
cfin	70kx0a9f\9051208.dat
cfout.txt	70kx0a9f\control.dat
cp6mfqbe.html	70kx0a9f\du44ugsd.dll
cxtpls_loader.exe	70kx0a9f\qz9dnjzs.dll
data.~	70kx0a9f\uj9s6igg.dll
dciatcha.exe	**********
dice21.ico	autoupdate\autoupdate.exe
edow_as2.exe	autoupdate\libexpat.dll
ei.exe	bullseye network\bin
exp.exe	bullseye network\ad.dat
ezl_kws[1].fcgi	bullseye network\ub.dat
farmmext.exe	bullseye network\uninstall.exe
free cell phone.ico	bullseye network\bin\adv.exe
free laptop computer.ico	bullseye network\bin\adx.exe
free picture ipod.ico	bullseye network\bin\bargains.exe
free ringtones!.ico	cashback\bin
free sony playstation.ico	cashback\ad.dat
free u2 ipod.ico	cashback\bb_auto_wider.swf
gogotoolssilawo19pi.exe	cashback\bb_click_wider.swf
greenmovie2313asaadsasfad.ico	cashback\bb_welcome.html
helper101.dll	cashback\bb_welcome1.swf
htisd.exe	cashback\blank.gif
i12.tmp	cashback\icon.gif
icejfjim.ini	cashback\logo.gif
id3.tmp	cashback\template.html
inst25[1].exe This is the	cashback\template2.html
wmplayer.exe.tmp	cashback\ub.dat
installer_marketing18.exe	cashback\uninstall.exe
io2uns.exe	cashback\bin\cashback.exe
itgbyf.exe	cashback\bin\cb.exe
javex80.vxd	cashback\bin\flash.exe
key.~	e2g\data19
log.~	e2g\iebhos.dll
mac80ex.idf	media pass\info.txt
mp3red51aads.ico	media pass\mediapass.exe
mqexdlm.srg	media pass\mediapassc.dll
msbe.dll	media pass\mediapassk.exe
nba giveaway.ico	mysearch\bar
nem220.dll	mysearch\bar\1.bin
netut80ex.vxd	mysearch\bar\cache
nsz81.dll	mysearch\bar\history
pacis.exe	mysearch\bar\settings
partypoker.com.ico	mysearch\bar\1.bin\mysearchpluginproxy.class
pcs_0008.exe	mysearch\bar\1.bin\npmysrch.dll
pi[1].exe	mysearch\bar\1.bin\s42ns.exe
pop up blaster1232131.ico	mysearch\bar\1.bin\s4bar.dll

pop2.exe
psis80ex.ax
ptf_0004.exe
ptf_0006.exe
ptf_0008.exe
q10pvbrv.dat
q17i9a4j.exe
q17i9a4j.ini
qh4mkbv9.dll
qqjjhvrt.exe
red_kas1.ico
ritsacnk.dat
rndrcus.exe
rqrkr.exe
rtneg2.dll
saie.exe
saie.log
sskcwrd.dll
sskknwrd.dll
sskuknwrd.dll
stubinst.exe
suicidetb.exe
thin-94-1-x-x.exe
thnall2c[1].exe
toc_0029.exe
toc_0032.exe
tool2_667279.exe
toz.exe
uoqg84qb.html
updlog355.exe
vcmnet9.exe
vh e2331.ico
vx0.nls
vx1.nls
vx1x.nls
vx2.nls
vx2x.nls
vx3.nls
vx3x.nls
windmy.dll
winnb57.dll
wintask.exe
winupdt.008
winupdt.bin
winupdt.exe

C:\ Temp is 180 solutions

C: \temp\fleok
C: \temp\bb_auto_wider.swf
C: \temp\bb_click_wider.swf
C: \temp\bb_welcome.html
C: \temp\bb_welcome1.swf
mysearch\bar\cache\0046847b
mysearch\bar\cache\00471159
mysearch\bar\cache\00477b3e.bmp
mysearch\bar\cache\0047ae2c.bmp
mysearch\bar\cache\files.ini
mysearch\bar\history\search
mysearch\bar\settings\prevcfg.htm
mysearch\surfsidekick 2\ssk.exe
mysearch\surfsidekick 2\sskbho.dll
mysearch\surfsidekick 2\sskcore.dll

IBIS websearch and its Toolbar

toolbar\cursors
toolbar\recordings
toolbar\skins
toolbar\update
toolbar\common.dll
toolbar\gykhxlmu.rmr
toolbar\iexploreskins.exe
toolbar\nzqlihv.wzg
toolbar\radio.exe
toolbar\tbps.exe
toolbar\toolbar.dll
toolbar\xlmurin.wzg
toolbar\yywr.wzg
toolbar\yywsv.wzg
toolbar\zwipvbh.wzg
toolbar\cursors\cursors.xml
toolbar\update\download

TopMoxie Ebates Mo Money

web_rebates\ap1150
web_rebates\da1150
web_rebates\sy1150
web_rebates\disp1150.exe
web_rebates\readme.txt
web_rebates\webrebates0.exe
web_rebates\webrebates1.exe
web_rebates\ap1150\merc1175.dat
web_rebates\ap1150\mercexcl.dat
web_rebates\ap1150\psid1175.dat
web_rebates\ap1150\topr1150.dat
web_rebates\da1150\pjordan
web_rebates\da1150\1150sh.dat
web_rebates\da1150\424cf968126f.dat
web_rebates\da1150\pjordan\424cf97f7ee8.dat
web_rebates\sy1150\html
web_rebates\sy1150\images
web_rebates\sy1150\sy1150
web_rebates\sy1150\tp1150
web_rebates\sy1150\html\f_popc1150c_rb.htm

C: \temp\blank.gif	web_rebates\sy1150\html\f_popo1150c_ub.htm
C: \temp\icon.gif	web_rebates\sy1150\html\f_spec1150c_rb.htm
C: \temp\logo.gif	web_rebates\sy1150\html\f_spec1150c_ub.htm
C: \temp\sahagent-cdt1004.exe	web_rebates\sy1150\html\foot1150c_rb.htm
C: \temp\salm.exe	web_rebates\sy1150\html\foot1150c_ub.htm
C: \temp\salm.log	web_rebates\sy1150\html\popo1150c.htm
C: \temp\salm_gdf.dat	web_rebates\sy1150\html\pref1150c.htm
C: \temp\salm_kyf.dat	web_rebates\sy1150\html\remv1150c.htm
C: \temp\salmau.dat	web_rebates\sy1150\html\scri1150a.htm
C: \temp\salmhook.dll	web_rebates\sy1150\html\spec1150c.htm
Local Settings\Temp	web_rebates\sy1150\images\p.gif
wrapperouter.exe	web_rebates\sy1150\images\topr_c_envelope.gif
ckz.tmp1eab22\gogotools-stealth.exe	web_rebates\sy1150\images\topr_c_footer.gif
ckz.tmp1eab22\silentinstallw32.exe	web_rebates\sy1150
drpc2.tmp\thnall2c.exe	\images\topr_c_hdr_autotrack_remove.gif
drtemp\wupdt.exe	web_rebates\sy1150\images\topr_c_hdr_settings.gif
	web_rebates\sy1150
	\images\topr_c_hdr_settings_toprebates.gif
	web_rebates\sy1150\images\topr_c_pop_circles.gif
	web_rebates\sy1150\images\topr_c_pop_circles_bg2.gif
	web_rebates\sy1150\images\topr_c_warning.gif
	web_rebates\sy1150\sy1150\1150_0.dat
	web_rebates\sy1150\sy1150\1150_1.dat
	web_rebates\sy1150\sy1150\1150_2.dat
	web_rebates\sy1150\tp1150\f_popo1150c_rb.htm
	web_rebates\sy1150\tp1150\f_popo1150c_ub.htm
	web_rebates\sy1150\tp1150\f_spec1150c_rb.htm
	web_rebates\sy1150\tp1150\f_spec1150c_ub.htm
	web_rebates\sy1150\tp1150\foot1150c_rb.htm
	web_rebates\sy1150\tp1150\foot1150c_ub.htm
	web_rebates\sy1150\tp1150\log.txt
	web_rebates\sy1150\tp1150\popo1150c.htm
	web_rebates\sy1150\tp1150\pref1150c.htm
	web_rebates\sy1150\tp1150\remv1150c.htm
	web_rebates\sy1150\tp1150\scri1150a.htm
	web_rebates\sy1150\tp1150\spec1150c.htm

This also installs the Transponder Gangs ceres.dll along with 2 new files and one has a registry entry in the HKey Current User.

download.abetterinternet.com/download/ahreco/ahreco.exe
static.abetterinternet.com/download/rndrcus/rndrcus.exe

Back to the Top

aHreco.exe
[HKEY_CURRENT_USER\Software\AHExe]
"AHI2d5OfSDist"="8|1|0|0|THIN-8-1-X-X.EXE"
"AHI2d5OfSInst"="{7C5B1C39-6E3D-4AA6-94B0-3CA8E8019232}"
"AHC2n5trMsgSDisp"=dword:00000025

"AHT2o5pListSPos"=dword:00000000
"AHs2t5icky1S"="lflshdt%3D1112338997%26istlogdt%3D20050401%26cb%3D%26cntp%3Dcable%26"
"AHs2t5icky2S"="0%3D%26fstcidt%3D1112338997103%26"
"AHs2t5icky3S"="0"
"AHs2t5icky4S"="0"
"AHC1o2d5eOfSFinalAd"="0"
"AHT2i5m9eOfSFinalAd"="0"
"AHD2s5tSSEnd"="'›–,ÀÀÍŸ›œ—ˆÁ□Š×›ƒ€□Š–›"'Ì'•,ÍŸ,À'—ˆ™Ž—Ž¸¯®Ž□•‡÷"
"AH2N5a9tionSCode"="US"
"AHP2D5om"="•‰„—ˆ€'†",‹ˆŸ□Ì'□Ÿ"
"AHT2h5rshSCheckSIn"=dword:0000002d
"AHT2h5rshSMots"=dword:00000064
"AHM2o5deSSync"=dword:0000000b
"AHI2n5ProgSCab"=dword:00000000
"AHI2n5ProgSEx"=dword:00000000
"AHI2n5ProgSLstest"=dword:00000000
"AHB2D5om"="›□‡†ŽŠ□›"›‡€"Š–Ü™€□Ž™ƒ‹™‰Á□€•"
"AHE2v5nt"="0"
"AHT2h5rshSBath"=dword:00002710
"AHT2h5rshSysSInf"=dword:000007d0
"AHL2n5Title"=dword:0000001e
"AHC2u5rrentSMode"=dword:00000001
"AHC2n5tFyl"=dword:00000000
"AHI2g5noreS"="™ƒ‹™‰
"AHS2t5atusOfSInst"="roger"
"AHL2a5stMotsSDay"=dword:00000001
"AHL2a5stSSChckin"=dword:00000ef1

Back up to File List **Back to the Top**

File Analysis

Clear Search new variants

****
3/31/ 4/1/2005 First infestation
C:\Program Files\70kx0a9f\70kx0a9f.exe
C:\Program Files\70kx0a9f\37353732.exe
O4 - HKLM\..\Run: [70kx0a9f] C:\Program Files\70kx0a9f\70kx0a9f.exe
****
70kx0a9f.exe
****
Version: 1.13.0.5
CRC-32: 0D87275C
MD5: EA465983DED888DF7C36630451D41F7B

Found in the code:
sds.clrsch.com/loader

****

7xwqsavz.DLL
****
Size: 147968
Version: 1.7.0.2
CRC-32: 60141BFF
MD5: E7E7EFAFDA1FE5621CBFA61FA8C0197D
Time stamp: Friday, April 01, 2005 2:11:06 AM
Creation: Friday, April 01, 2005 2:11:06 AM
Last access: Saturday, December 30, 1899 12:00:00 AM
Last write: Friday, April 01, 2005 2:11:06 AM

Version
File version: 1, 7, 0, 2
Company name: ClearSearch
Internal name: LoaderUpdater
Original filename: LoaderUpdater.dll
Product name: ClearSearch LoaderUpdater
Product version: 1, 7, 0, 2
File description: LoaderUpdater

Update: 2 April 2005 10:57 PM EST

Windows Media Player wmplayer.exe.tmp Exploit

Finally found where the wmplayer.exe.tmp exploit file came from and the file that created it!

pan-advert.com/ads/banners//inst25.exe - **This is the wmplayer.exe.tmp**
inst25.exe 5kb
wmplayer.exe.tmp in windows media player folder
code:
adlinstallwin32.exe /system32/adlinstallwin32.exe SystemRoot wb
alwaysupdatednews.com/terms/ toc_0032.exe
**
inst25.exe 5kb in Temp Internet files folder
code:
adlinstallwin32.exe /system32/adlinstallwin32.exe SystemRoot wb
alwaysupdatednews.com/terms/ toc_0032.exe

Back up to File List **Back to the Top**

Now pan-advert.com has an email to aviabiz.com and the address in the whois for aviabiz.com is the same address in the whois for pacimedia.com.

Whois Data

pan-advert.com 213.159.119.4
Registrant:
Sea Media S.A. Sea Media S.A. seamedia @aviabiz.com
Sea Media S.A.
P.O. Box 1987 9A
Panama NONE NA

PA
507-575-6771
Domain Name: pan-advert.com
Admin Contact:
Zarya Econsulting Corp. Zarya Econsulting Corp. info@aviabiz.com
P.O. Box 1987 9A
Panama NA
PA
507-575-6771
Technical Contact:
Sea Media S.A Sea Media S.A info@aviabiz.com
Sea Media S.A
P.O. Box 1987 9A
Panama NA
PA
507-575-6771
Billing Contact:
Sea Media S.A Sea Media S.A info@aviabiz.com
Sea Media S.A
P.O. Box 1987 9A
Panama NA
PA
507-575-6771
Record created on Jan 4 2005.
Record expires on Jan 4 2006.
Domain servers:
ns1.pan-advert.biz
ns2.pan-advert.biz
**
pacimedia.com 213.159.119.18

Domain name: pacimedia.com
Administrative Contact:
-
Tomaz Urbic pacerdltd@yahoo.com
1.2069844492
Fax: -
Trinity House 1st Floor
Albert Street PO BOX 1402
Victoria MAHE N/A
SC
Billing Contact:
-
Tomaz Urbic pacerdltd@yahoo.com
1.2069844492
Fax: -
Trinity House 1st Floor
Albert Street PO BOX 1402
Victoria MAHE N/A
SC
Technical Contact:

-
Tomaz Urbic pacerdltd@yahoo.com
1.2069844492
Fax: -
Trinity House 1st Floor
Albert Street PO BOX 1402
Victoria MAHE N/A
SC
Registrant Contact:
-
Tomaz Urbic pacerdltd@yahoo.com
1.2069844492
Fax: -
Trinity House 1st Floor
Albert Street PO BOX 1402
Victoria MAHE N/A

aviabiz.com 204.118.173.14
Registrant:
Zarya Econsulting Corp. Zarya Econsulting Corp. info@aviabiz.com
Trinity house 1st Floor Albert Street P.O. BOX 1402
Victoria Mahe NA
SC
206-666-3972
Domain Name: aviabiz.com
Admin Contact:
Zarya Econsulting Corp. Zarya Econsulting Corp. info@aviabiz.com
Trinity house 1st Floor Albert Street P.O. BOX 1402
Victoria Mahe NONE NA
SC
206-666-3972
Technical Contact:
Zarya Econsulting Corp. Zarya Econsulting Corp. info@aviabiz.com
Trinity house 1st Floor Albert Street P.O. BOX 1402
Victoria Mahe NONE NA
SC
206-666-3972
Billing Contact:
Zarya Econsulting Corp. Zarya Econsulting Corp. info@aviabiz.com
Trinity house 1st Floor Albert Street P.O. BOX 1402
Victoria Mahe NONE NA
SC
206-666-3972
Record created on Jan 12 2004.
Record expires on Jan 12 2006.
Domain servers:
ns1.abc-hosts.com
ns2.abc-hosts.com

Back to the Top

| **Home** | **Main Menu** |