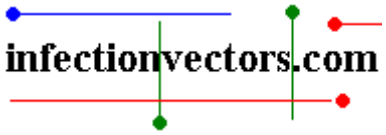


Beagle.BG-BJ/Mitglieder (Tooso) Propagation
infectionvectors.com
March 2005

The Beagle variants released March 1, 2005 used a specialized means of propagation that allows the author much greater control over the malware. This report outlines how the latest copies of the Beagle worm and its companion Trojan found their way to thousands of machines during the first few days of March 2005. As will be shown, the Beagle creator employed this strategy in August of 2004 with the AO variant.

The initial mass mailing for this round of Beagle variants was a well-seeded attack that simply mailed the Trojan commonly known as Tooso in the following example message:

```
To:          [Recipient]
From:        [Spoofed]
Subject:     [Blank]
Attachment: new_price.zip
Message:     price
```

The worm reaches out to the following web address to retrieve email addresses to target with copies of the Trojan: http://oceancareers.com/z/sss2.php.

Once opened, the ZIP archive reveals a single executable, for example, "doc_43.exe," which installs the Trojan on the local machine. The Trojan works much earlier copies of Mitglieder did with Beagle.AO (from August of 2004). It was emailed with very similar email subjects and attachment names. Furthermore, the same entry was made in the compromised machine's Registry to ensure that the code auto started with the operating system (using the value "Ru1n"). For more information on AO see the second part of the Beagle History trilogy.

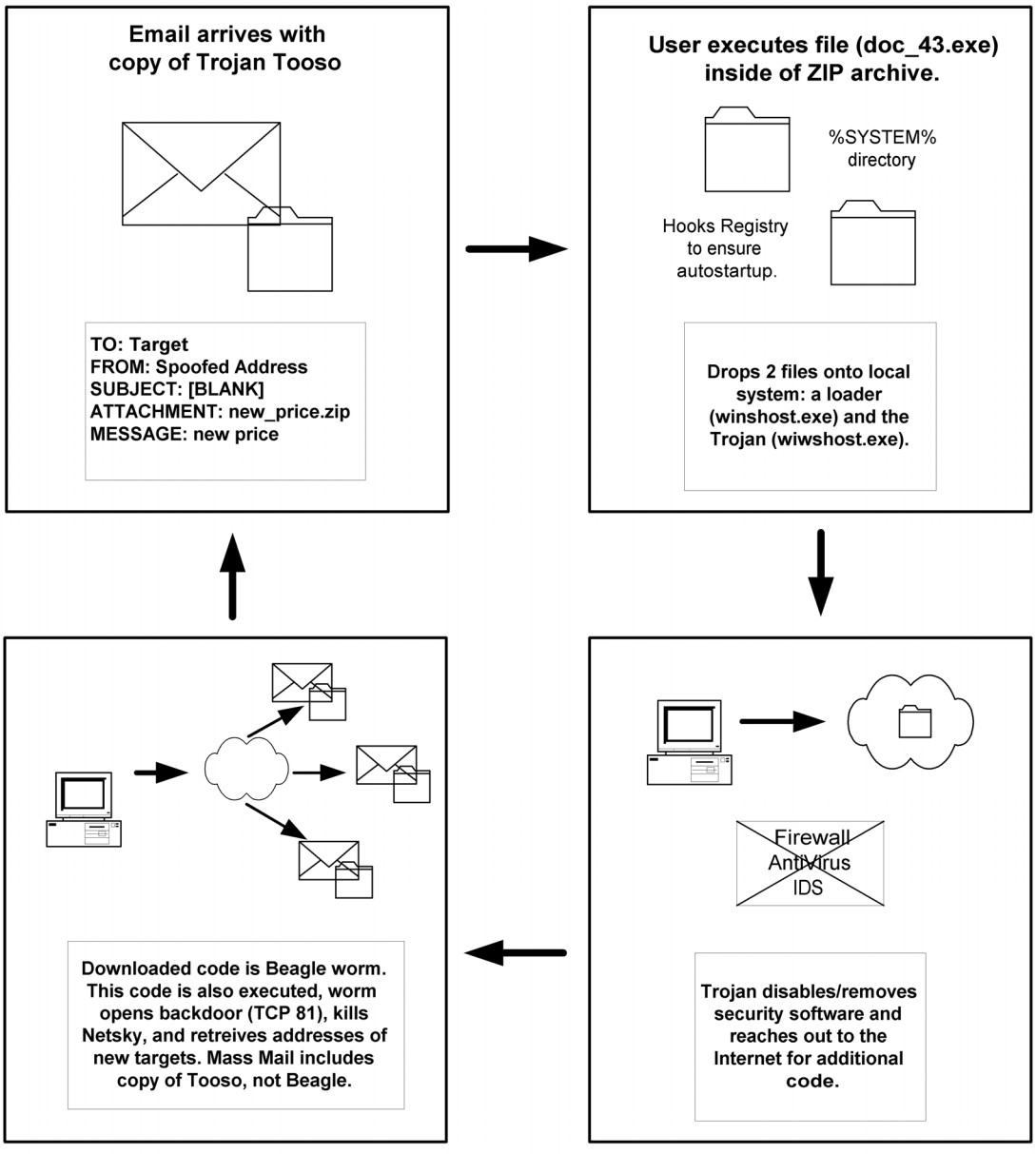
The strategic advantage this provides is the ability to stay ahead of anti-virus software for an extended period of time. As the anti-virus vendors release signatures to detect one of the components, the author can modify the code (as simple as repacking the PE) so that the new method is ineffective. As Kaspersky analyst Yury Mashevsky noted on the Viruslist.com blog (http://www.viruslist.com/en/weblog March 1, 2005):

```
Moreover, today we have already intercepted 15 new pieces of malware
produced by the authour of Bagle. The newest variants follow hard on
the heels of our updates and we suspect that the authour is creating
new variants every time we release updates to block previous versions.
```

The use of this model was very successful for the AO variant, and the release of 4 versions of each (both the worm and the Trojan) on March 1, 2005 led to a number of infections for the BG-BJ iterations. The diagram below explains the propagation method:

Beagle.BG-BJ Propagation

Examples are from Tooso/Beagle.BG samples received 01 March 2005.



Additional Information About the Trojan Mitglieder/Tooso:

In order to download the file "zo2.jpg" (saved as "_re_file.exe") the Trojan calls the import: urlmon.URLDownloadToFileA for a long list of servers, all of which are currently unavailable (1 March 2005). This is a familiar tactic of the Beagle author who routinely waits weeks in some cases before posting the additional files.

The following strings output shows the antivirus/firewall/intrusion prevention processes hunted by Beagle.BG:

AVXQUAR.EXE
ESCANHNT.EXE
UPGRADER.EXE
AVXQUAR.EXE
AVWUPD32.EXE
AVPUPD.EXE
CFIAUDIT.EXE
UPDATE.EXE
NUPGRADE.EXE
MCUPDATE.EXE
ATUPDATER.EXE
AUPDATE.EXE
AUTOTRACE.EXE
AUTOUPDATE.EXE
FIREWALL.EXE
ATUPDATER.EXE
LUALL.EXE
DRWEBUPW.EXE
AUTODOWN.EXE
NUPGRADE.EXE
OUTPOST.EXE
ICSSUPPNT.EXE
ICSUPP95.EXE
ESCANH95.EXE

The Registry values/keys deleted by this malware:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,Symantec NetDriver Monitor
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,ccApp
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,NAV CfgWiz
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,SSC_UserPrompt
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,McAfee Guardian
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,McAfee.

InstantUpdate.Monitor

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,APVXDWIN
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,KAV50
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,avg7_cc
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,avg7_emc
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,Zone Labs Client
HKLM\SOFTWARE\Symantec
HKLM\SOFTWARE\McAfee
HKLM\SOFTWARE\KasperskyLab
HKLM\SOFTWARE\Agnitum
HKLM\SOFTWARE\Panda Software
HKLM\SOFTWARE\Zone Labs

The HOSTS file entries written by the Trojan:

127.0.0.1 localhost
127.0.0.1 ad.doubleclick.net
127.0.0.1 ad.fastclick.net
127.0.0.1 ads.fastclick.net
127.0.0.1 ar.atwola.com
127.0.0.1 atdmt.com
127.0.0.1 avp.ch
127.0.0.1 avp.com
127.0.0.1 avp.ru
127.0.0.1 awaps.net
127.0.0.1 banner.fastclick.net
127.0.0.1 banners.fastclick.net
127.0.0.1 ca.com
127.0.0.1 click.atdmt.com
127.0.0.1 clicks.atdmt.com
127.0.0.1 dispatch.mcafee.com
127.0.0.1 download.mcafee.com
127.0.0.1 download.microsoft.com
127.0.0.1 downloads.microsoft.com
127.0.0.1 engine.awaps.net
127.0.0.1 fastclick.net
127.0.0.1 f-secure.com
127.0.0.1 ftp.f-secure.com
127.0.0.1 ftp.sophos.com
127.0.0.1 go.microsoft.com
127.0.0.1 liveupdate.symantec.com
127.0.0.1 mast.mcafee.com
127.0.0.1 mcafee.com
127.0.0.1 media.fastclick.net
127.0.0.1 msdn.microsoft.com
127.0.0.1 my-etrust.com

127.0.0.1 nai.com
127.0.0.1 networkassociates.com
127.0.0.1 office.microsoft.com
127.0.0.1 phx.corporate-ir.net
127.0.0.1 secure.nai.com
127.0.0.1 securityresponse.symantec.com
127.0.0.1 service1.symantec.com
127.0.0.1 sophos.com
127.0.0.1 spd.atdmt.com
127.0.0.1 support.microsoft.com
127.0.0.1 symantec.com
127.0.0.1 update.symantec.com
127.0.0.1 updates.symantec.com
127.0.0.1 us.mcafee.com
127.0.0.1 vil.nai.com
127.0.0.1 viruslist.ru
127.0.0.1 windowsupdate.microsoft.com
127.0.0.1 www.avp.ch
127.0.0.1 www.avp.com
127.0.0.1 www.avp.ru
127.0.0.1 www.awaps.net
127.0.0.1 www.ca.com
127.0.0.1 www.fastclick.net
127.0.0.1 www.f-secure.com
127.0.0.1 www.kaspersky.ru
127.0.0.1 www.mcafee.com
127.0.0.1 www.my-etrust.com
127.0.0.1 www.nai.com
127.0.0.1 www.networkassociates.com
127.0.0.1 www.sophos.com
127.0.0.1 www.symantec.com
127.0.0.1 www.trendmicro.com
127.0.0.1 www.viruslist.ru
127.0.0.1 ftp://ftp.kasperskylab.ru/updates/
127.0.0.1 ftp://ftp.avp.ch/updates/
127.0.0.1 http://www.kaspersky.ru/updates/
127.0.0.1 http://updates1.kaspersky-labs.com/updates/
127.0.0.1 http://updates3.kaspersky-labs.com/updates/
127.0.0.1 http://updates4.kaspersky-labs.com/updates/
127.0.0.1 http://updates2.kaspersky-labs.com/updates/
127.0.0.1 http://updates5.kaspersky-labs.com/updates/
127.0.0.1 http://downloads1.kaspersky-labs.com/updates/
127.0.0.1 http://www.kaspersky-labs.com/updates/
127.0.0.1 ftp://updates3.kaspersky-labs.com/updates/
127.0.0.1 ftp://downloads1.kaspersky-labs.com/updates/
127.0.0.1 www3.ca.com

127.0.0.1 ids.kaspersky-labs.com
127.0.0.1 downloads2.kaspersky-labs.com
127.0.0.1 downloads1.kaspersky-labs.com
127.0.0.1 downloads3.kaspersky-labs.com
127.0.0.1 downloads4.kaspersky-labs.com
127.0.0.1 liveupdate.symanteclive update.com
127.0.0.1 liveupdate.symantec.com
127.0.0.1 update.symantec.com
127.0.0.1 download.mcafee.com
127.0.0.1 www.symantec.com
127.0.0.1 securityresponse.symantec.com
127.0.0.1 symantec.com
127.0.0.1 www.sophos.com
127.0.0.1 sophos.com
127.0.0.1 www.mcafee.com
127.0.0.1 mcafee.com
127.0.0.1 liveupdate.symanteclive update.com
127.0.0.1 www.viruslist.com
127.0.0.1 viruslist.com
127.0.0.1 f-secure.com
127.0.0.1 www.f-secure.com
127.0.0.1 kaspersky.com
127.0.0.1 kaspersky-labs.com
127.0.0.1 www.avp.com
127.0.0.1 www.kaspersky.com
127.0.0.1 avp.com
127.0.0.1 www.networkassociates.com
127.0.0.1 networkassociates.com
127.0.0.1 www.ca.com
127.0.0.1 ca.com
127.0.0.1 mast.mcafee.com
127.0.0.1 my-etrust.com
127.0.0.1 www.my-etrust.com
127.0.0.1 download.mcafee.com
127.0.0.1 dispatch.mcafee.com
127.0.0.1 secure.nai.com
127.0.0.1 nai.com
127.0.0.1 www.nai.com
127.0.0.1 update.symantec.com
127.0.0.1 updates.symantec.com
127.0.0.1 us.mcafee.com
127.0.0.1 liveupdate.symantec.com
127.0.0.1 customer.symantec.com
127.0.0.1 rads.mcafee.com
127.0.0.1 trendmicro.com
127.0.0.1 www.trendmicro.com

127.0.0.1 www.grisoft.com

The following services are also killed by the Trojan:

wuauserv
PAVSRV
PAVFNSVR
PSIMSVC
Pavkre
PavProt
PREVSRV
PavPrSrv
SharedAccess
navapsvc
NPFMntor
Outpost Firewall
SAVScan
SBService
Symantec Core LC
ccEvtMgr
SNDSrvc
ccPwdSvc
ccSetMgr.exe
SPBBCSvc
KLBLMain
avg7alrt
avg7updsvc
vsmon
CAISafe
avpcc
fsbwsys
backweb client - 4476822
backweb client-4476822
fsdfwd
F-Secure Gatekeeper Handler Starter
KAVMonitorService
navapsvc
NProtectService
Norton Antivirus Server
VexiraAntivirus
dvpinit
dvpapi
schscnt
BackWeb Client - 7681197
F-Secure Gatekeeper Handler Starter
AVPCC

KAVMonitorService
Norman NJeeves
NVCScheduler
nvcoas
Norman ZANDA
PASSRV
SweepNet
SWEEPSRV.SYS
NOD32ControlCenter
NOD32Service
PCCPFW
Tmntsrv
AvxIni
XCOMM
ravmon8
SmcService
BlackICE
PersFW
McAfee Firewall
OutpostFirewall
NWService
alerter
sharedaccess
NISUM
NISSERV
vsmon
nwclnth
nwclntg
nwclnte
nwclntf
nwclntd
nwclntc
wuauserv
navapsvc
Symantec Core LC
SAVScan
kavsvc
DefWatch
Symantec AntiVirus Client
NSCTOP
Symantec Core LC
SAVScan
SAVFMSE
ccEvtMgr
navapsvc
ccSetMgr

VisNetic AntiVirus Plug-in
McShield
AlertManger
McAfeeFramework
AVExch32Service
AVUPDService
McTaskManager
Network Associates Log Service
Outbreak Manager
MCVSRte
mcupdmgr.exe
AvgServ
AvgCore
AvgFsh
awhost32
Ahnlab task Scheduler
MonSvcNT
V3MonNT
V3MonSvc
FSDFWD

Finally, any local file with a name matching one of the following strings will be deleted:

mysuperprog.exe
CCSETMGR.EXE
CCEVTMGR.EXE
NAVAPSVC.EXE
NPFMNTOR.EXE
symlcsvc.exe
SPBBCSvc.exe
SNDSrvc.exe
ccApp.exe
ccl30.dll
ccvrtrst.dll
LUALL.EXE
AUPDATE.EXE
Luupdate.exe
LUINSDLL.DLL
RuLaunch.exe
CMGrdian.exe
Mcshield.exe
outpost.exe
Avconsol.exe
Vshwin32.exe
VsStat.exe
Avsynmgr.exe

kavmm.exe
Up2Date.exe
KAV.exe
avgcc.exe
avgemc.exe
zonealarm.exe
zatutor.exe
zlavscan.dll
zlclient.exe
isafe.exe
cafix.exe
vsvault.dll
av.dll
vetredir.dll
C1CSETMGR.EXE
CC1EVTMGR.EXE
NAV1APSVC.EXE
NPFM1NTOR.EXE
s1ymlcsvc.exe
SP1BBCSvc.exe
SND1Srvc.exe
ccA1pp.exe
cc1l30.dll
ccv1rtrst.dll
LUAL1L.EXE
AUPD1ATE.EXE
Luup1date.exe
LUI1NSDLL.DLL
RuLa1unch.exe
CM1Grdian.exe
Mcsh1ield.exe
outp1ost.exe
Avc1onsol.exe
Vshw1in32.exe
Vs1Stat.exe
Av1synmgr.exe
kav12mm.exe
Up222Date.exe
K2A2V.exe
avgc3c.exe
avg23emc.exe
zonealarm.exe
zatutor.exe
zlavscan.dll
zo3nealarm.exe
zatu6tor.exe

zl5avscan.dll
zlcli6ent.exe
is5a6fe.exe
c6a5fix.exe
vs6va5ult.dll
a5v.dll
ve6tre5dir.dll

The Trojan reaches out via the following addresses to retrieve additional code (included for research and monitoring purposes, visit at one's own risk):

http://www.amanit.ru/zo2.jpg
http://www.anthonyflanagan.com/zo2.jpg
http://www.approved1stmortgage.com/zo2.jpg
http://www.argument.h12.ru/zo2.jpg
http://www.arkebek.de/zo2.jpg
http://www.artek.org/zo2.jpg
http://www.asianfestival.nl/zo2.jpg
http://www.astergut.at/zo2.jpg
http://www.aviation-center.de/zo2.jpg
http://www.bbsh.org/zo2.jpg
http://www.besino.com/zo2.jpg
http://www.bestbuy.de/zo2.jpg
http://www.beta.mtw.ru/zo2.jpg
http://www.bga-gsm.ru/zo2.jpg
http://www.blessino.com/zo2.jpg
http://www.blueeyeinc.com/zo2.jpg
http://www.breaklight.be/zo2.jpg
http://www.brzesko.net.pl/zo2.jpg
http://www.catsystem.com.kg/zo2.jpg
http://www.cdnpartner.com.pl/zo2.jpg
http://www.ceskyhosting.cz/zo2.jpg
http://www.channeland.com/zo2.jpg
http://www.compsolutionstore.com/zo2.jpg
http://www.concept.kg/zo2.jpg
http://www.corpsite.com/zo2.jpg
http://www.couponcapital.net/zo2.jpg
http://www.DarrkSydebaby.com/zo2.jpg
http://www.dehut-westerhoven.nl/zo2.jpg
http://www.dhl.kg/zo2.jpg
http://www.dierollendedisco.de/zo2.jpg
http://www.discobaradventure.be/zo2.jpg
http://www.e-nfo.com/zo2.jpg
http://www.e-power.com.cn/zo2.jpg
http://www.ecobank.kg/zo2.jpg

http://www.elenalazar.com/zo2.jpg
http://www.epicbiz.com/zo2.jpg
http://www.europa.kg/zo2.jpg
http://www.everett.wednet.edu/zo2.jpg
http://www.externet.hu/zo2.jpg
http://www.forester.kg/zo2.jpg
http://www.fotocliparts.de/zo2.jpg
http://www.fotonw.org/zo2.jpg
http://www.freesites.com.br/zo2.jpg
http://www.funbunker.de/zo2.jpg
http://www.funworld.tv/zo2.jpg
http://www.gameser.com@share.gameser.com/zo2.jpg
http://www.gci-bln.de/zo2.jpg
http://www.gcnet.ru/zo2.jpg
http://www.giantrevenue.com/zo2.jpg
http://www.himpsi.org/zo2.jpg
http://www.i3dvr.com/zo2.jpg
http://www.ibigmart.net/zo2.jpg
http://www.idb-group.net/zo2.jpg
http://www.illusionoflife.net/zo2.jpg
http://www.infocuspromo.com/zo2.jpg
http://www.irinaswelt.de/zo2.jpg
http://www.jansenboiler.com/zo2.jpg
http://www.jasnet.pl/zo2.jpg
http://www.jcribeiro.com/zo2.jpg
http://www.jewelleryamberproducts.com/zo2.jpg
http://www.jimvann.com/zo2.jpg
http://www.jldr.ca/zo2.jpg
http://www.jordanramey.net/zo2.jpg
http://www.joy-musik-sound.de/zo2.jpg
http://www.justrepublicans.com/zo2.jpg
http://www.katel.kg/zo2.jpg
http://www.knicks.nl/zo2.jpg
http://www.koebers.pl/zo2.jpg
http://www.kogaionon.com/zo2.jpg
http://www.kplus.kg/zo2.jpg
http://www.kradtraining.de/zo2.jpg
http://www.kranenberg.de/zo2.jpg
http://www.kranenberg.de:113547@/zo2.jpg
http://www.kstrus.com.pl/zo2.jpg
http://www.ktsonline.de/zo2.jpg
http://www.lahelaino.com/zo2.jpg
http://www.lawform.com.au/zo2.jpg
http://www.leetexgroup.com/zo2.jpg
http://www.leshrak.de/zo2.jpg
http://www.leshrak.de:prophets@/zo2.jpg

http://www.logoseiten.de/zo2.jpg
http://www.magicbottle.com.tw/zo2.jpg
http://www.mcuserver.cz/zo2.jpg
http://www.mega-spass.com/zo2.jpg
http://www.mega.kg/zo2.jpg
http://www.mepbisu.de/zo2.jpg
http://www.mepmh.de/zo2.jpg
http://www.mtfdesign.com/zo2.jpg
http://www.mtransit.kg/zo2.jpg
http://www.neotech.kg/zo2.jpg
http://www.nikonfotoshare.com/zo2.jpg
http://www.novosti.kg/zo2.jpg
http://www.ok.kg/zo2.jpg
http://www.onepositiveplace.org/zo2.jpg
http://www.online.kg/zo2.jpg
http://www.orangesuburban.5u.com/zo2.jpg
http://www.otv.ch/zo2.jpg
http://www.pageantpage.com/zo2.jpg
http://www.pankration.com/zo2.jpg
http://www.para-agility.com/zo2.jpg
http://www.pdxracing.net/zo2.jpg
http://www.pfadfinder-leobersdorf.com/zo2.jpg
http://www.pipni.cz/zo2.jpg
http://www.pjwstk.edu.pl/zo2.jpg
http://www.polizeimotorrad.de/zo2.jpg
http://www.proway-consulting.com/zo2.jpg
http://www.pugetsoundyc.org/zo2.jpg
http://www.pyrlandia-boogie.pl/zo2.jpg
http://www.qphoto.co.za/zo2.jpg
http://www.raecoinc.com/zo2.jpg
http://www.realgps.com/zo2.jpg
http://www.realty.kg/zo2.jpg
http://www.redlightpictures.com/zo2.jpg
http://www.reliance-yachts.com/zo2.jpg
http://www.relocationflorida.com/zo2.jpg
http://www.rentalstation.com/zo2.jpg
http://www.rieraquadros.com.br/zo2.jpg
http://www.roaming.kg/zo2.jpg
http://www.sacohalle.be/zo2.jpg
http://www.scanex-medical.fi/zo2.jpg
http://www.scoping4success.com/zo2.jpg
http://www.sert.ru/zo2.jpg
http://www.sigi.lu/zo2.jpg
http://www.spadochron.pl/zo2.jpg
http://www.ssc.kg/zo2.jpg
http://www.ssmifc.ca/zo2.jpg

http://www.stadtmeyers.de/zo2.jpg
http://www.stadtmeyers.de:R2D2c3po@/zo2.jpg
http://www.sterlingirb.com/zo2.jpg
http://www.sunassetholdings.com/zo2.jpg
http://www.szantomierz.art.pl/zo2.jpg
http://www.szosa.pl/zo2.jpg
http://www.tambourenvereine.ch/zo2.jpg
http://www.tarnow.opoka.org.pl/zo2.jpg
http://www.tc-muraene.com/zo2.jpg
http://www.tc-muraene.com:hunter@/zo2.jpg
http://www.theroyalregistry.com/zo2.jpg
http://www.transportation.gov.bh/zo2.jpg
http://www.tumar.kg/zo2.jpg
http://www.tunguska.hu/zo2.jpg
http://www.turkeyhomes.com/zo2.jpg
http://www.turkeyhomes.com@/zo2.jpg
http://www.ulpiano.org/zo2.jpg
http://www.unicity.pl/zo2.jpg
http://www.vbw.info/zo2.jpg
http://www.velezcourtesymanagement.com/zo2.jpg
http://www.vorrix.com/zo2.jpg
http://www.webpark.pl/zo2.jpg
http://www.wecompete.com/zo2.jpg
http://www.wp.pl/zo2.jpg
http://www.wwwebad.com/zo2.jpg
http://www.xpager321.wz.cz/zo2.jpg
http://www.yamdiamonds.com/zo2.jpg
http://www.zander-yachting.com/zo2.jpg