



Search

< < <

Tuesday, January 6, 2009

> > >

MAIN INDEX

ARCHIVES

ABOUT US

SECURITY CENTER

SUBMIT SAMPLE

BETA LABS

LINUX BLOG

eSTORE

BE SURE.

MS08-067 Worms

Posted by Mikko @ 18:15 GMT |

Over the last days, we've received reports of corporate networks getting infected with various variants of **MS08-067** worms. These are mostly **Downadup/Conficker** variants.

The malware uses server-side polymorphism and ACL modification to make network disinfection particularly difficult. A sign of infection is that user accounts become locked out of an Active Directory domain as the worm attempts to crack account passwords using a built-in dictionary. When it fails, it leads to those accounts being locked.

We have detailed information about the malware functionality in [our Downadup.AL description](#).

We also have a separate tool available to assist in disinfecting. The tool is available from [here](#).

We also recommend system administrators to block access to web sites used by the worm. The sites keep changing, but the current domains to block are:

acqggcq.cn
adbsq.net
akgjmdzx.cc
bclaxb.cn
bdjtrpaav.cc
bdrmpudqh.cn
boirczdikw.com
bpufhbvwjws.com
bwocsfviu.net
bwtrd.net
bxtopike.ws
ccgdllgwkw.info
ccolbxddud.com
cdbhi.cn
cfcipqz.biz
ciopicmfq.info
cjeyj.com
crikr.cn
dbizknbfyv.cn
dckhrrqh.com
djthknbtxe.cc
dkvjxac.info
dphxqdp.cn
drykouwoa.com
dugnyfnxky.com
dwiknmnhx.org
esujw.cn
eufiwwkplyc.cn
evtwdavi.net
evuqysnc.cc
ezkhbz.org
fhchak.org
fhioqvdpdg.info
fhoptkn.org
fjxkmq.ws
fnmhkizip.ws
fnopiz.cn
fnxklfyxdy.com
gdneutxoi.cc
girirvjy.org
govagjcasyo.cn
gqjgx.cn
gwfnepcus.ws
hbkbc.biz
hpmhoassp.org
hrmwzqif.com
hwmggrmzdsw.biz
hxhpc.org
ibifq.ws
icbabdoo.org
igggellu.ws
imaexvImjn.org
ipuuulsw.com
itiuv.cn
itzbanmjbds.ws
iuqmkmlklbw.ws
jfqlrlgf.biz
jilpumzn.ws
jldifsh.net
jnfcmuhfum.ws
jpgflwtu.net
jqlmcfmdua.info
jqmdyemnd.cn
jufwmttx.net
jzvspdcv.cn

kbrlxkiohfb.org
kcawyfgl.ws
kkvugfb.biz
knpfuq.cc
ktveyekd.cn
kuiq.org
kxsmffcsh.biz
lejhfcdm.biz
leyloenk.cc
lmcrkcuu.net
lrkewik.net
lrwnqgoj.biz
memsvr.com
miyga.biz
mmpfans.ws
mxvrtq.net
nhmgtrmka.org
nmdrr.com
nqnmjn.org
nwczo.cc
nykyhzap.cc
oawtwovet.cc
oecsw.net
omxanan.ws
ovqoluqwhf.org
pakzqankxai.ws
pnaeydmg.org
pvfivnqgk.cn
qauaiepfih.ws
qdgvbkipopx.net
qhdefcfkqg.cc
qtjumbvk.ws
quvjfczmd.net
qvuycgw.net
qwwnsrgii.cn
qxdzbtgok.org
rcoesjhii.info
rrtvw.org
sedueat.cc
siirkijx.cn
sjarftss.biz
snytwwp.cc
srfvt.com
srtbuvesjmy.org
thzydzvunfk.biz
tlxjjlmk.org
tmegbpwamyr.ws
tnaqhezhsww.biz
tsamlnes.cc
txibddqtpuj.cc
udthrtx.cc
udyxa.info
uikrcuzw.com
uuuwlcpzi.cn
vbvvhgs.net
vfdjkunysp.cn
vhgppqfiga.cc
vlfk.info
vrfouwsk.net
vuvjptke.org
vxuiwtpqc.info
vxuuur.biz
wagwovomnj.net
wbpciauakl.ws
wdgeaqrhk.net
weekax.cn
wpnmravf.cc
wycqkpn.cn
xakcypzbi.org
xbrpaahhcl.org
xbtqz.com
xfpzmkcl.cc
xgdgxusdq.org
xihpmics.net
xrbczsuyw.com
xyywekmbuuq.net
yagcjzafet.cn
yjslycn.org
ykzoap.cc
yrmek.cc
yrmvbwbzlt.ws
yryxdaecqwa.info
ysuxkcv.com
ywictoyhzeu.ws
zajmcwcknwn.biz
zfrcc.org
zjcmnmrpwdp.info
zrfdubsgmuq.net
ztyshleh.biz

We'll update this list as needed.

Update: Additional details can be found [here](#).

Comments

