



On the Kraken and Bobax Botnets

Paul Royal
April 9, 2008

Purpose

This document provides a discussion of the Kraken botnet's relationship to the Bobax botnet.

1. Kraken, Bobax and Layer 8

Damballa's announcement of Kraken has garnered concerns from other organizations in the information security industry, some of whom feel that Kraken was misrepresented as "new." Others have made even stronger statements, saying that Damballa has "repackaged Bobax" and presented it as Kraken [1]. Damballa's initial disclosure says only that "Kraken was first observed in winter 2007, but investigation into its origins suggests the existence of early variants as far back as late 2006 [2]." So is Kraken new? Damballa believes it is, but the process of looking for an answer goes deeper than a simple definition of term and it highlights an important and more general problem.

The heart of the issue deals with the way information security professionals identify and categorize different entities based on their available sources and their organization's focus. Some companies focus on spamming and deal strictly with spam data. To these companies, a distinct entity (and its size) is defined as a group created by their clustering algorithms, which perform grouping using many attributes of spam data (e.g., the contents of a message body or how a victim acts as an SMTP engine). This perspective is different but still meaningful, because it can be corroborated with other data sources (or data views) to make "*Layer 8*" connections—social or political connections that relate technical entities to a common person or group of people.

As an example, consider the case where the results of clustering show that two known separate botnets appear as a single botnet according to spam data. A security researcher could conclude that while the botnets are separate, *they are likely controlled or were created by the same group*. This discovery is a Layer 8 connection and, briefly extending the example, it could help law enforcement coordinate its efforts by associating what were previously thought to be two unrelated sets of evidence.

The aforementioned example is highly analogous to concerns expressed by other professionals in regards to the "newness" of Kraken and its relationship to Bobax [1,3]. Specifically, several organizations have leveraged their expertise in malware analysis to confirm the presence of a Layer 8 connection [3,4,6]. Damballa has subsequently confirmed this Layer 8 (common author or group) connection, and a brief survey showing *why* Bobax is different from Kraken is in order.

Debuting in 2004, Bobax (like Kraken) was a large, spamming botnet. Similar to Kraken, Bobax used Dynamic DNS (DDNS) providers ChangeIP, DynServ, Yi, and others. Completely unlike

Kraken (which encrypts all communication with the CnC and communicates on UDP and TCP port 447), Bobax used *plaintext HTTP* for communicating with the CnC. Yet, just like Kraken, Bobax used the same domain name generation algorithm, although the domains for Kraken (Appendix A) are completely disjoint from the domains for Bobax (Appendix B). The following table summarizes the two botnets' similarities and differences:

	Bobax	Kraken
DDNS Providers	Similar to Kraken; did not use DynDNS	Similar to Bobax, does not use ChangeIP
Domain Names	Common generation algorithm but different (completely disjoint) domain names	Common generation algorithm but different (completely disjoint) domain names
CnC Protocol	Plaintext HTTP	Encrypted UDP/TCP 447

In his 2004 analysis of Bobax, Joe Stewart stated that an examination of the inner-workings of Bobax showed enough similarities to other spam trojans (e.g., Minit) to infer that “This could be an indication that they at least share some of the same code if they are not written by the same author [5].” Mr. Stewart was using his malware analysis expertise to remark on a possible Layer 8 connection, which is exactly what organizations like ThreatExpert [4] or SANS ISC [3] recently reported about Kraken. That is, they have made compelling discoveries that suggest code reuse or a common author between *two different spamming botnets that use different CnC domains and a fundamentally different CnC protocol*.

[1] http://blog.washingtonpost.com/securityfix/2008/04/kraken_creates_a_clash_of_the.html

[2] <http://www.cnbc.com/id/23993105>

[3] <http://isc.sans.org/diary.html?storyid=4256>

[4] <http://blog.threatexpert.com/2008/04/crikey-youve-been-kraken.html>

[5] <http://www.secureworks.com/research/threats/bobax/>

[6] <http://www.secureworks.com/research/threats/topbotnets/>

Appendix A: Kraken CnC Domain Names

aafsytdyndns.org	fvivkenao.dyndns.org	jydgkodyndns.org
aetqzvfzub.dyndns.org	fxhbaxmuakb.dyndns.org	kbhtmpyw.dyndns.org
aifuunhoomc.dyndns.org	gdqnofcwvim.dyndns.org	kczuuykc.dyndns.org
akuqejwvztx.dyndns.org	gfzcpunx.dyndns.org	kdxrydhtbw.dyndns.org
axlime.dyndns.org	ggdcnsp.dyndns.org	kmmpqogwh.dyndns.org
baqydcdnusq.dyndns.org	ghcxncadnj.dyndns.org	kmrbok.dyndns.org
bayqvt.dyndns.org	gmqaeoedhd.dyndns.org	kpjobheecz.dyndns.org
bdzxcl.dyndns.org	gmsaxtqrn.dyndns.org	kpzlenrn.dyndns.org
bezmabz.dyndns.org	gnkovlb.dyndns.org	krqdnikw.dyndns.org
bfhagswbf.dyndns.org	gqwxcgusq.dyndns.org	ksxqzyfsnif.dyndns.org
bjjdhgpbby.dyndns.org	gyuzohut.dyndns.org	kwdgnbrodtx.dyndns.org
bnbnpqkagr.dyndns.org	gzezryargx.dyndns.org	kymniq.dyndns.org
bqzzqwwi.dyndns.org	hdzonujenwv.dyndns.org	kzcpywbfjee.dyndns.org
bvvliba.dyndns.org	hicsac.dyndns.org	lbbnllfno.dyndns.org
bwmcuzdurhk.dyndns.org	hjavglrwd.dyndns.org	lfqbim.dyndns.org
bxlginh.dyndns.org	hmhauqssekwyndns.org	likkxhbl.dyndns.org
cczxqasliks.dyndns.org	hnkoso.dyndns.org	lkgdxi.dyndns.org
cipaxqmcgfh.dyndns.org	hpnitjssj.dyndns.org	lkhilzwbv.dyndns.org
cvvhgffch.dyndns.org	hrlgrh.dyndns.org	llkzijizw.dyndns.org
cyytqnxx.dyndns.org	htlosdk.dyndns.org	llmqjmx.dyndns.org
dakxslvxy.dyndns.org	huslbscekh.dyndns.org	lquely.dyndns.org
danssxjggqh.dyndns.org	ibfxdlyzdm.dyndns.org	lraxjgzdggv.dyndns.org
dftinvludyndns.org	iefavv.dyndns.org	lslxgkyn.dyndns.org
djealpwhf.dyndns.org	iffefnn.dyndns.org	lulpkc.dyndns.org
dkflxkqecdf.dyndns.org	ihcvduav.dyndns.org	majzshaqgfs.dyndns.org
dmaciltbek.dyndns.org	ijycaynckx.dyndns.org	manoscjm.dyndns.org
doqsstt.dyndns.org	ikbjwyhy.dyndns.org	mcomsm.dyndns.org
dqovzm.dyndns.org	imhdouaxqg.dyndns.org	mdfwebqw.dyndns.org
dvguqvob.dyndns.org	imuwutyqtti.dyndns.org	mfffwqk.dyndns.org
dztvxvpt.dyndns.org	ipgcyhufwqw.dyndns.org	mquiuaodyndns.org
echxfsqy.dyndns.org	ivybjwxblai.dyndns.org	mqwjwoyuyf.dyndns.org
ehlskzmg.dyndns.org	izucjnv.dyndns.org	mvcjpbjbydyndns.org
elvzol.dyndns.org	jegztaw.dyndns.org	mvkhwpcnog.dyndns.org
emoudfytxou.dyndns.org	jejyiqw.dyndns.org	mxdovclldv.dyndns.org
eobpyvk.dyndns.org	jgmpwk.dyndns.org	nageynise.dyndns.org
erzmjlcg.dyndns.org	jhgtyzb.dyndns.org	naihpmfx.dyndns.org
esbdeicjwmx.dyndns.org	jjmiak.dyndns.org	nbbbxjvmyg.dyndns.org
esycuzpqq.dyndns.org	jnhmue.dyndns.org	nbtqzhloxw.dyndns.org
etrzubdna.dyndns.org	jnwvchqcr.dyndns.org	ndbpxddj.dyndns.org
ezynefc.dyndns.org	jolpfzruup.dyndns.org	ndgmklb.dyndns.org
fdsnwrcrtjnh.dyndns.org	jskzox.dyndns.org	njcwnaug.dyndns.org
flegrzjott.dyndns.org	jslkra.dyndns.org	nnfhfbt.dyndns.org
fmjkijeamgp.dyndns.org	jtbotmb.dyndns.org	nnhbqapa.dyndns.org
fousax.dyndns.org	jvayxqd.dyndns.org	noikukdz.dyndns.org
fsnjcfg.dyndns.org	jvcgmc.dyndns.org	nsrdnx.dyndns.org
ftepfemhyp.dyndns.org	jvpjotuiogn.dyndns.org	nsuiajj.dyndns.org

nthtvsyswq.dyndns.org	ucnsdljylvb.dyndns.org	novbsmekge.dyndns.org
nukrwdbfsxv.dyndns.org	ucyfhq.dyndns.org	zsakypru.dyndns.org
odibaxefav.dyndns.org	ueyyjniofd.dyndns.org	ebbnzqx.dyndns.org
olojojgzyc.dyndns.org	uiyqugayqbx.dyndns.org	tkmhpnthfsz.dyndns.org
oonliui.dyndns.org	uqsxiq.dyndns.org	szbagncpev.dyndns.org
oqqqjve.dyndns.org	uresesbfsb.dyndns.org	jnetgzttxsk.dyndns.org
ovcueg.dyndns.org	uuqbjuz.dyndns.org	srusvher.dyndns.org
ovdvzqu.dyndns.org	uydsxnill.dyndns.org	fvecgexi.dyndns.org
ozpojgbssm.dyndns.org	vfbbeshdoej.dyndns.org	lmfbjndkqd.dyndns.org
pbqfzoryej.dyndns.org	vfcomwakbs.dyndns.org	qtexhg.dyndns.org
pccnjhluxl.dyndns.org	vpqvwvqmdz.dyndns.org	bylkpy.dyndns.org
pcygte.dyndns.org	vwvfauos.dyndns.org	nckndnu.dyndns.org
pwoyexstvw.dyndns.org	vzzbeamwie.dyndns.org	ycofnn.dyndns.org
pwrbxafiyhf.dyndns.org	wabuku.dyndns.org	atgoycu.dyndns.org
qsxhvbwuf.dyndns.org	wbmmppbjf.dyndns.org	ckwkklamspio.dyndns.org
rffcteo.dyndns.org	wcnemwndx.dyndns.org	xzpknuvovk.dyndns.org
rfhsatwliv.dyndns.org	wfzfrhanjc.dyndns.org	jhfqjyek.dynserv.com
rhxqccwdhwg.dyndns.org	wkyohk.dyndns.org	akdkin.dynserv.com
rjbboc.dyndns.org	wpvdbwyzc.dyndns.org	gzhhhlb.dynserv.com
rjlymb.dyndns.org	wvqzgyfkasp.dyndns.org	hsbyswcyqgk.dynserv.com
rjukvyfrkw.dyndns.org	wwkgpfiz.dyndns.org	ahlpxy.dynserv.com
rlygbcjevix.dyndns.org	xawpaoq.dyndns.org	adrxokqn.dynserv.com
rlxnpfwypys.dyndns.org	xcmmpwylghk.dyndns.org	gbsszmdkuq.dynserv.com
rmgwqurk.dyndns.org	xkayuxlvs.dyndns.org	fyeldg.dynserv.com
rpupaji.dyndns.org	xlrtlmam.dyndns.org	vjxpdyv.dynserv.com
rqmpbii.dyndns.org	xmynlzgp.dyndns.org	xckzkip.dynserv.com
rsawfg.dyndns.org	xorjoet.dyndns.org	vtdddxys.dynserv.com
rsxhoojs.dyndns.org	xoweqtscuy.dyndns.org	ebksscgcdd.dynserv.com
rxsqqcss.dyndns.org	xwnlbfcpmmv.dyndns.org	vddlysri.dynserv.com
sfhksfw.dyndns.org	yappjfassl.dyndns.org	uvbvdmocd.dynserv.com
sjxhzwvtj.dyndns.org	ybilwkaz.dyndns.org	anrgxq.dynserv.com
smpyfxs.dyndns.org	ymcotzrr.dyndns.org	nvhjzbp.dynserv.com
smwytfqyde.dyndns.org	ymunqnlcw.dyndns.org	nvnxznygos.dynserv.com
spycoqeywmk.dyndns.org	ysyzetd.dyndns.org	hshfmrobjfr.dynserv.com
sqnkiz.dyndns.org	yxjanpevse.dyndns.org	jlpswkv.dynserv.com
sransxyzp.dyndns.org	zjcquwl.dyndns.org	tkoappwny.dynserv.com
stxzbnll.dyndns.org	zkhfah.dyndns.org	uqgxsl.dynserv.com
sxjotx.dyndns.org	zmdohcpex.dyndns.org	oadcqaqr.dynserv.com
szbrht.dyndns.org	zongrwt.dyndns.org	uposzmce.dynserv.com
tghebo.dyndns.org	zuvzbnq.dyndns.org	oaioaojp.dynserv.com
thgpkqh.dyndns.org	adrcgmzrm.dyndns.org	ocjvlbqs.dynserv.com
tjptbtrbgke.dyndns.org	lfiavsbyntu.dyndns.org	xqgonbfwye.dynserv.com
tkhgti.dyndns.org	iskqszufrrt.dyndns.org	ocqkgmoa.dynserv.com
tlkrqxbtj.dyndns.org	mszbnhwhzhvv.dyndns.org	odaqaqkttm.dynserv.com
tnifpmeh.dyndns.org	xnzkdos.dyndns.org	uokvzojl.dynserv.com
toafns.dyndns.org	vsdzee.dyndns.org	zpuxyczd.dynserv.com
toauarcnave.dyndns.org	dkbjzbq.dyndns.org	ulssrxrzu.dynserv.com
trjrvmgbxya.dyndns.org	nmuzqnexl.dyndns.org	ogplkaktknb.dynserv.com

tsvhsh.dyndns.org	zkfxpvc.dyndns.org	ujlzcmejhn.dynserv.com
ftchmggp.dynserv.com	jzgpwo.dynserv.com	rnfcpaixdmt.dynserv.com
ojgxqhr.dynserv.com	xkttdu.dynserv.com	kpnohhzt.dynserv.com
uifrrmhyg.dynserv.com	sjkjtfaqj.dynserv.com	wmoutza.dynserv.com
jmyyptoo.dynserv.com	pxihdssdnvb.dynserv.com	hnmgivqndrk.dynserv.com
eihasiwowm.dynserv.com	kassfz.dynserv.com	egglqna.dynserv.com
cqdzsbdy.dynserv.com	qebihodgxqv.dynserv.com	kqllwrovaeb.dynserv.com
ucxibbeenwz.dynserv.com	seqzgkytg.dynserv.com	gqybspk.dynserv.com
iikctrpa.dynserv.com	yknskhnrjs.dynserv.com	inzaqdtputo.dynserv.com
cazrsihs.dynserv.com	gxbeemxaiz.dynserv.com	cbcmbxvbsrh.dynserv.com
tvzggexcvfv.dynserv.com	scmltb.dynserv.com	ksxvcfy.dynserv.com
orhsnoiv.dynserv.com	qijoywreqq.dynserv.com	ktcieq.dynserv.com
orkkmyromi.dynserv.com	qkdqentrif.dynserv.com	eczhhaj.dynserv.com
ormmasflo.dynserv.com	rzfowocrt.dynserv.com	kuhzahg.dynserv.com
ttykgsdq.dynserv.com	qljpnkbjij.dynserv.com	xtuuqvgfbi.dynserv.com
osvfjswcnn.dynserv.com	qmnnxv.dynserv.com	dzsjniwffrx.dynserv.com
xoskcy.dynserv.com	ezflrfh.dynserv.com	dzammohbly.dynserv.com
koaqnn.dynserv.com	qmuuqyb.dynserv.com	dxcbdx.dynserv.com
ddrqyggw.dynserv.com	kcarwyggmp.dynserv.com	gnmmpxb.dynserv.com
bodrxb.dynserv.com	qqoxxop.dynserv.com	kyurpkcmr.dynserv.com
jpbytzo.dynserv.com	qrquota.dynserv.com	yoriulioeo.dynserv.com
hovdworcxd.dynserv.com	rokjemchbd.dynserv.com	dwlkloufb.dynserv.com
zyaquzholfi.dynserv.com	ykvzjuq.dynserv.com	wirmkbbkikk.dynserv.com
yivdetzqvs.dynserv.com	xmbryakrity.dynserv.com	iqozgozb.dynserv.com
eoiovsq.dynserv.com	ewahbzgw.dynserv.com	ypscls.dynserv.com
pdduitmqhzj.dynserv.com	kfqbbqx.dynserv.com	lbkhtebgit.dynserv.com
pdfaswmn.dynserv.com	qtoftdrsbx.dynserv.com	dsbhsflxfc.dynserv.com
tjgpkvvtob.dynserv.com	xttjdfir.dynserv.com	drdioqdjho.dynserv.com
pepntatkq.dynserv.com	rnfmtpiet.dynserv.com	dpjrhvxy.dynserv.com
frcgwebfwmh.dynserv.com	qxsaxoacg.dynserv.com	doxokpbliuz.dynserv.com
titstvez.dynserv.com	qyjceavgdsq.dynserv.com	dldhzpphgw.dynserv.com
jqwnnincq wz.dynserv.com	rbltobttor.dynserv.com	xhhifkm.dynserv.com
pspypf.dynserv.com	gugjymmo.dynserv.com	irurmiseo.dynserv.com
uaqjtycx.dynserv.com	rcrwuqtcmmf.dynserv.com	isxxozigv.dynserv.com
ycbfpeyae.dynserv.com	rdlenr.dynserv.com	djlfsmj.dynserv.com
huqtjcatrf.dynserv.com	kjiyoh.dynserv.com	itnofebo.dynserv.com
ydxbzl.dynserv.com	kkodsmudw.dynserv.com	lgzieppr.dynserv.com
wygjimewotz.dynserv.com	wtmnwhh.dynserv.com	rcruohsseib.dynserv.com
swxxkyi.dynserv.com	huwoyvagozu.dynserv.com	ljjldhdshf.dynserv.com
stingvr.dynserv.com	wqwttk.dynserv.com	diyermz.dynserv.com
ilrmjjuz.dynserv.com	cfcsndquwjc.dynserv.com	dqiqi.dynserv.com
cwrrdxye.dynserv.com	rijvir.dynserv.com	itytizvqdf.dynserv.com
dljemwae.dynserv.com	kmubffne.dynserv.com	dhievgx.dynserv.com
yisqdvqg.dynserv.com	rjevqixpsjs.dynserv.com	dgbxzfz.dynserv.com
jyylmnmvx.dynserv.com	epvskyare.dynserv.com	dfyyyopbyzf.dynserv.com
ptlaig.dynserv.com	eonrrqeu.dynserv.com	llklvlubj.dynserv.com
slkxchc.dynserv.com	ensnijibic.dynserv.com	yshrdp.dynserv.com
jzdwbfir.dynserv.com	rluxdhubir.dynserv.com	ysiefvjp.dynserv.com

ptzjyxymqof.dynserv.com	endfyjc.dynserv.com	llzvkwmxh.dynserv.com
putphxczr.dynserv.com	ymikwrqrrg.dynserv.com	xgyllfmhtyv.dynserv.com
hnukbxx.dynserv.com	vrybipcapn.dynserv.com	yabpedfs.mo00.com
lotyzvchnn.dynserv.com	mxzszjtac.dynserv.com	jixiqvsguut.mo00.com
hyoiwjx.dynserv.com	xdbxaaf.dynserv.com	jlbkzpjgn.mo00.com
vvjfsj.dynserv.com	gestlmvmjqq.dynserv.com	jlqpeujbjbp.mo00.com
ytgvyywx.dynserv.com	bafirop.dynserv.com	yauhoxb.mo00.com
hctrgy.dynserv.com	axxubqahlae.dynserv.com	ybgcei.mo00.com
ytkvvuknpt.dynserv.com	vcpcnqi.dynserv.com	jqbcxu.mo00.com
xoogblws.dynserv.com	urgfiluop.dynserv.com	jqkjkz.mo00.com
dbtteg.dynserv.com	hrwxno.dynserv.com	ydedcqpdble.mo00.com
hawkhllexk.dynserv.com	vriurfuzfrx.dynserv.com	yhzdldtofq.mo00.com
dbsoal.dynserv.com	awzzsd.dynserv.com	jzzyjaiede.mo00.com
ytskykvn.dynserv.com	gejqvonji.dynserv.com	kbrzkkq.mo00.com
gvgqpueeq.dynserv.com	nghhezqyrfy.dynserv.com	ymbepny.mo00.com
iyiznt.dynserv.com	nhalhad.dynserv.com	khufndoqpz.mo00.com
wbgoeu.dynserv.com	atxkjarv.dynserv.com	kiingoc.mo00.com
lwrjmu.dynserv.com	zkupsly.dynserv.com	klmtord.mo00.com
gmkxtm.dynserv.com	aqixuwkwudv.dynserv.com	ymmsztgnb.mo00.com
lygvassxij.dynserv.com	xpmsjptzw.dynserv.com	krpruobbtcn.mo00.com
wbfwrrrjo.dynserv.com	xydjuwfft.dynserv.com	ynfqicvvyqr.mo00.com
lytyicrge.dynserv.com	ammnifbseja.dynserv.com	kunjbkpp.mo00.com
cyiiejrr.dynserv.com	gbtpyjs.dynserv.com	yohhiu.mo00.com
lzvuyqiom.dynserv.com	vqqcfigm.dynserv.com	lawzaa.mo00.com
yueire.dynserv.com	hnkypvj.mo00.com	lfreyzkr.mo00.com
makpvgrpm.dynserv.com	hpapprvyh.mo00.com	lfwftbtdgjh.mo00.com
cpmqekpse.dynserv.com	humbjatp.mo00.com	lfwjkwa.mo00.com
gkenyoabmg.dynserv.com	hwrnjis.mo00.com	lgqlhy.mo00.com
iziavxznp.dynserv.com	hyffjoxbrq.mo00.com	lkuekdxbofy.mo00.com
ciliejchzm.dynserv.com	hzxghrpsxv.mo00.com	lmfviji.mo00.com
gjrszcz.dynserv.com	icixemu.mo00.com	lnbyesrxp.mo00.com
cditpjxmgdy.dynserv.com	icspdih.mo00.com	loyalneu.mo00.com
izlwodgff.dynserv.com	idzhbmy.mo00.com	lrcxtd.mo00.com
aqtxloupefy.dynserv.com	xpnbsq.mo00.com	lszxxnw.mo00.com
gzwqowjpk.dynserv.com	igoygdf.mo00.com	lugzmfms.mo00.com
jbnsnx.dynserv.com	xqkpcbort.mo00.com	lunajs.mo00.com
giyscw.dynserv.com	xrbxpl.mo00.com	lvdnbnwmai.mo00.com
vyrizkpu.dynserv.com	ilcbcsxdk.mo00.com	lwsqwnzom.mo00.com
ghmelx.dynserv.com	immanrynlap.mo00.com	yuwzsixzuh.mo00.com
mqctckevqpj.dynserv.com	inlwntrol.mo00.com	mcotackq.mo00.com
brrpirqixi.dynserv.com	inxxkp.mo00.com	medhtzj.mo00.com
vxfbmdnlph.dynserv.com	ivhhct.mo00.com	ywlacvk.mo00.com
bpjiclpp.dynserv.com	ivodajlpp.mo00.com	mhqbszalsp.mo00.com
xmhbwd.dynserv.com	xuxsczv.mo00.com	mhxdfu.mo00.com
bosxrhq.dynserv.com	iwxjwww.mo00.com	minkoq.mo00.com
mvxsyyrs.dynserv.com	ixoynk.mo00.com	momktjnclgk.mo00.com
mwadqdc.dynserv.com	iybexlxx.mo00.com	yyxrelchaix.mo00.com
bmycoj.dynserv.com	xvczzlgflrn.mo00.com	zcxutl.mo00.com

mwpqscj.dynserv.com	jednsq.mooo.com	zeltgapu.mooo.com
bhebfod.dynserv.com	jfjklejmbyj.mooo.com	nfldevwga.mooo.com
bgrerl.dynserv.com	jgewisqg.mooo.com	nfopvf.mooo.com
nlnylxvrbel.mooo.com	riilslp.mooo.com	vfojcgop.mooo.com
nmcptmxkg.mooo.com	kbblmkbe.mooo.com	vistifggmc.mooo.com
oycruzxouli.mooo.com	evudfvve.mooo.com	vjwvlyba.mooo.com
zmwmxnfvw.mooo.com	ovsddwubkz.mooo.com	vmfnrgw.mooo.com
npckycdf.mooo.com	dauhiasf.mooo.com	agaghdert.mooo.com
nprnrxl.mooo.com	zxglzfhu.mooo.com	agdwsptbxo.mooo.com
nroxkspoq.mooo.com	rmahrf.mooo.com	ankoiutx.mooo.com
nsikcrl.mooo.com	rzdpmgfwoh.mooo.com	aotpsivloe.mooo.com
nsscsq.mooo.com	xyqpaw.mooo.com	apbmswjqbz.mooo.com
nvxptqurlqu.mooo.com	ycjesqgj.mooo.com	aqlmngwgupn.mooo.com
nwyqq.mooo.com	ftytgfehid.mooo.com	arrcwsn.mooo.com
ocniqqtmio.mooo.com	rsstzff.mooo.com	atxjwtq.mooo.com
oiixtyhfgm.mooo.com	krjkfnsqsh.mooo.com	vrvbzymuku.mooo.com
zrlxqlflhtm.mooo.com	ruxujk.mooo.com	vrvdhlui.mooo.com
oovvkgo.mooo.com	fxmbsrue.mooo.com	bbhgylu.mooo.com
opndfi.mooo.com	ryvenskbbk.mooo.com	vsidaikx.mooo.com
ouancdi.mooo.com	rzxoiewf.mooo.com	bfszvjrsvt.mooo.com
patwcfb.mooo.com	safbvvgortr.mooo.com	bhimcgfl.mooo.com
pazduvpgg.mooo.com	sapgvql.mooo.com	bissgm.mooo.com
zyjdvjihz.mooo.com	sbbvnpms.mooo.com	bjisvur.mooo.com
pfyxqhanw.mooo.com	scttfzou.mooo.com	booxl.mooo.com
phxmlhbw.mooo.com	videfgkn.mooo.com	boushimkvog.mooo.com
piswagkygc.mooo.com	sgnsygczki.mooo.com	bpofpvndwml.mooo.com
plsckrw.mooo.com	quowesuqbbb.mooo.com	btewjdhkxk.mooo.com
pnpcbmfvhui.mooo.com	slbrrevv.mooo.com	btjsiqg.mooo.com
pnuzje.mooo.com	qfrgvbmowr.mooo.com	buecrxhtoo.mooo.com
pofkqvd.mooo.com	snkgth.mooo.com	bxfubiiq.mooo.com
prifhjstv.mooo.com	dcdkfq.mooo.com	ccrdlxflo.mooo.com
pstjjafdb.mooo.com	stznid.mooo.com	cfbcpqzz.mooo.com
ptjzkbpmnvp.mooo.com	sunnpcnsw.o.mooo.com	cfprocus.mooo.com
ptxmmkgr.mooo.com	swsmyvc.mooo.com	chqycawqy.mooo.com
pwlpzrylrun.mooo.com	sxoogybzgfv.mooo.com	ckvzxmcm.mooo.com
zzhbrvtxeiu.mooo.com	sxormxaqthj.mooo.com	clbypsvp.mooo.com
pzpizg.mooo.com	csukibyyt.mooo.com	cvfrdr.mooo.com
qgrdscyf.mooo.com	tdxjkeeutb.mooo.com	wammrsuhayk.mooo.com
qgtqwxjwmiw.mooo.com	thpwkd.mooo.com	cwbsenvtcr.mooo.com
qmqbwnyzewa.mooo.com	cmviueadnal.mooo.com	dablid.mooo.com
qqkxdhw.mooo.com	iwstvwv.mooo.com	drpwkpijsp.mooo.com
sfsocnwdnw.mooo.com	trppywlyuf.mooo.com	smgojbhuyw.mooo.com
qtdmcra.mooo.com	tsbvewputv.mooo.com	ebdqxgnm.mooo.com
qteaali.mooo.com	tuoswxeoqlw.mooo.com	efwmtpedgyy.mooo.com
qtkbjdx.mooo.com	tzvhyc.mooo.com	emdunxqvjvf.mooo.com
quqozf.mooo.com	ufdwpvgvj.mooo.com	eoxjsnvzuh.mooo.com
rckyibrjmrw.mooo.com	ykrzcragnnu.mooo.com	esbwimya.mooo.com
revvpzuuv.mooo.com	unjghufx.mooo.com	zztsqfzsbdb.mooo.com

tjetqly.mo00.com	uqmwgucn.mo00.com	evnmcjcbj.mo00.com
rjxnpjf.mo00.com	uvsbzwj.mo00.com	evyharj.mo00.com
rhpstjtlwdm.mo00.com	uzxnneqh.mo00.com	fhavrcvziql.mo00.com
znkhrtojwx.mo00.com	vedrtwtyw.mo00.com	fhfaronxx.mo00.com
wyyozskwecl.mo00.com	niyqqfxygly.yi.org	byrubffha.yi.org
wzmdmzfht.mo00.com	avlgaoar.yi.org	calovhzpsv.yi.org
fpeirgwhxjs.mo00.com	avsyzltsjqp.yi.org	jhafczshwfv.yi.org
xapjjfglotq.mo00.com	nfluntl.yi.org	mhctdivn.yi.org
ftotupatsxp.mo00.com	nflhsmjjuh.yi.org	cdbcqqtzluc.yi.org
fuodqqxsdz.mo00.com	axpehmx.d.yi.org	mfaovpr.yi.org
fvcpbtsk.mo00.com	zgvxgm.yi.org	cdocrguwf.yi.org
fwisyzp.mo00.com	zfmheud.yi.org	cehxrq.yi.org
fxsigsvhyjz.mo00.com	pcajqcaof.yi.org	ceuswc.yi.org
fybjazu.mo00.com	xtlczgyi.yi.org	xpewycmkui.yi.org
gacpcwgwd.mo00.com	bbblhiks.yi.org	cfbpsdxtijt.yi.org
gbtdmaomtr.mo00.com	gxoebjd.yi.org	xlfstaxlrui.yi.org
gbviejbs.mo00.com	bbnmuuscwm.yi.org	chdgoxpfs.yi.org
xcvbmaxkrt.mo00.com	bdubefoeg.yi.org	jftkte.yi.org
xfkixgpjlq.mo00.com	mxybuuvfjzi.yi.org	chznlw.yi.org
gjewqe.mo00.com	ilwclwblahl.yi.org	yvmhvap.yi.org
xhlmrrbs.mo00.com	vutpaq.yi.org	itifvo.yi.org
gotlokmbwvh.mo00.com	jtkktuow.yi.org	wyudom.yi.org
gqtmrgtbkak.mo00.com	zctyzkvlosi.yi.org	hbqfqs.yi.org
guwyaqagyz.mo00.com	mwqgwuqu.yi.org	cngavndedml.yi.org
gwfmg.h.mo00.com	fwaxdmjesfh.yi.org	cnrrizbhhm.yi.org
hadgfilg.mo00.com	bhrxmwhjs.yi.org	coypkaecyz.yi.org
hfltemaw.mo00.com	bhtioi.yi.org	cpiqfey.yi.org
hinqarp.mo00.com	bibgwzvuy.yi.org	yuvuhsw.yi.org
hjbqfyg.mo00.com	iklnafi.yi.org	csoyrmxiti.yi.org
hjntjfyeqe.mo00.com	bjdpms.yi.org	xvyfxxcyym.yi.org
xnklfsjst.mo00.com	xcloyln.yi.org	cvkeykvgas.yi.org
hmhxnpk.mo00.com	vwernpcpt.yi.org	hzlicyml.yi.org
hmruxtb.mo00.com	mwgoefg.yi.org	jcoklydzugy.yi.org
hmsaqrsft.mo00.com	gwyziux.yi.org	cybckpcx.yi.org
nqpsra.yi.org	boabspnkjt.yi.org	lzpmyedjxgi.yi.org
vpjfkambi.yi.org	ixyznn.yi.org	waxmtzkqblh.yi.org
iocfyfsc.yi.org	zafkgweeyic.yi.org	czeeqgntkfd.yi.org
yhwvatobnk.yi.org	fyaztpmd.yi.org	gisskw.yi.org
nqomncagfch.yi.org	bpiqfld.yi.org	l.yi.org
qwzsprieo.yi.org	yxnsgtbegg.yi.org	lwftjabdsb.yi.org
nokhexd.yi.org	bpnfqu.yi.org	lulolog.yi.org
zmhibanctbq.yi.org	icrnotkqj.yi.org	ltazldrfyxz.yi.org
altaebb.yi.org	bqsjinwewi.yi.org	ddaota.yi.org
amesjik.yi.org	bqulma.yi.org	iqwifsunu.yi.org
nmpmdyj.yi.org	mqnrmjv.yi.org	ldddjb.yi.org
andcuaylu.yi.org	cdggua.yi.org	lkxdrhqml.yi.org
imyonl.yi.org	jjetvmoptq.yi.org	dqfboc.yi.org
xnxvojpl.yi.org	hmoeuufk.yi.org	lkwxpj.yi.org

hovhgwralt.yi.org	yaczxxxg.yi.org	dijmji.yi.org
nkpynonh.yi.org	vygmudq.yi.org	yreoqmpaog.yi.org
jqwldiwvlv.yi.org	mkabjj.yi.org	yqzzag.yi.org
gxalwq.yi.org	halizxn.yi.org	yqcoqgmmb.yi.org
jltvmwdwoj.yi.org	vywyvdtksc.yi.org	lghuuuvwoct.yi.org
zssdxcq.yi.org	bpdyttrlp.yi.org	ufizpvq.yi.org
yqahgfox.yi.org	emjyyhsnfs.yi.org	ufkoityecy.yi.org
whnvfm.yi.org	snzftfdwr.yi.org	okoovh.yi.org
dmnffduljev.yi.org	psrjan.yi.org	hgswylecgom.yi.org
wibausx.yi.org	wmvrpvpqqu.yi.org	ogvfpx.yi.org
dowiqzh.yi.org	psoqzsgmd.yi.org	uktzmm.yi.org
ldwtlokyxa.yi.org	pqthoq.yi.org	odzsjiq.yi.org
lduizfn.yi.org	zvfctvkdng.yi.org	undubayt.yi.org
wiqblsfx.yi.org	kongwnop.yi.org	kfbldccj.yi.org
drclpvmt.yi.org	kolnvtddihu.yi.org	odbcdkeg.yi.org
ldttufo.yi.org	svezhitljis.yi.org	oadtbtlv.yi.org
jbwcodf.yi.org	svljrmqr.yi.org	oactsvt.yi.org
lcfcezeqq.yi.org	svwqgaovce.yi.org	kbyqffm.yi.org
dtixnbyuey.yi.org	enzfccit.yi.org	qpyosxkmcc.yi.org
rmeuuyino.yi.org	pqetatz.yi.org	nylskdky.yi.org
qwiglir.yi.org	pkkkepdyg.yi.org	urriekfm.yi.org
rnozsqygfk.yi.org	eoagag.yi.org	zpdygcp.yi.org
roisnge.yi.org	wpsfihxwh.yi.org	zpaqcybvni.yi.org
qsesrrwefp.yi.org	kofudwhje.yi.org	uvjvvpjl.yi.org
laebdbppt.yi.org	tdtccdfb.yi.org	ezmpfzfglt.yi.org
dvwyrgkjr.yi.org	iuiqjzqrlwx.yi.org	uwsyasugjdp.yi.org
dwfbta.yi.org	gvailawmc.yi.org	udtwirqzhdm.yi.org
kzdogza.yi.org	tgzbdfdprh.yi.org	wvvirkbn.yi.org
kxtdcnxinjm.yi.org	hzmwxlmu.yi.org	vcwivqhy.yi.org
kwkctaymrmk.yi.org	knzvnunfpy.yi.org	nteribmo.yi.org
rxgczwbyhvq.yi.org	pgjlls.yi.org	tqrvhfsdlup.yi.org
dzbzgittmwd.yi.org	pdmtvipa.yi.org	nszxnvwz.yi.org
ryqprkiu.yi.org	zzaanssdc.yi.org	zosxgnqe.yi.org
ynizzrrao.yi.org	tjzvboqqef.yi.org	feuafskvegb.yi.org
qkeienrl.yi.org	ymhthnfdq.yi.org	vhmhhxdcj.yi.org
dvbutsrzrgw.yi.org	tljzib.yi.org	fhabqjlbh.yi.org
izlpyrpbjo.yi.org	zxfutqtbncu.yi.org	hrhfevkmkun.yi.org
ebowzzw.yi.org	muodaclf.yi.org	njjiwilpnt.yi.org
wljknf.yi.org	zxkcat.yi.org	fhwqikf.yi.org
sbsuzkh.yi.org	zwhutmqv.yi.org	vvnvfrjxtpq.yi.org
qgvwxzw.yi.org	gdrhlg.yi.org	vouwbqfi.yi.org
ktggxfhmkfk.yi.org	iqubqksbudz.yi.org	
qgcyyogo.yi.org	klkkwdwzqco.yi.org	
sfbxsg.yi.org	tsjoiwyhmc.yi.org	
iyobnny.yi.org	klofmvcx.yi.org	
sglrundy.yi.org	osfnzykv.yi.org	
kqgcvvv.yi.org	hqedhgimgz.yi.org	
ngbmfsbuql.yi.org	zswiqpmcsxw.yi.org	

sjriqtnzq.yi.org	etwyr.s.yi.org	
sjwdfzvo.yi.org	opqhfeb.yi.org	
wmbmobl.yi.org	opjkkihbm.yi.org	
kpwyhgci.yi.org	zrvpvlzyoky.yi.org	
ptntsmg.yi.org	dstgrg.yi.org	
iyjofi.yi.org	iptwga.yi.org	

Appendix B: Bobax CnC Domain Names

dlivmg.1dumb.com	mhnyavmf.afraid.org	yraqztt.hn.org
eivysjix.1dumb.com	pkvgzaeca.afraid.org	yrztpzjou.hn.org
fndvrix.1dumb.com	pkvgzaecagx.afraid.org	dgwigom.yi.org
glilepv.1dumb.com	qbycxpxz.afraid.org	exrjbc.yi.org
gyssafaiq.1dumb.com	qqycilcd.afraid.org	ezqqddbkc.yi.org
iyruptr.1dumb.com	qujuvukbvbc.afraid.org	fcnhysydw.yi.org
kkjekaoii.1dumb.com	sbjuixfbjvk.afraid.org	gtyeywobh.yi.org
kvuznwxmfoj.1dumb.com	wyqggvow.afraid.org	iogrdedv.yi.org
mfltoqqgt.1dumb.com	yjtuvsro.afraid.org	kpxvrvde.yi.org
mgoelz.1dumb.com	cwkeyw.dynserv.com	kpxvrvdefs.yi.org
qeqfsvxous.1dumb.com	fzddik.dynserv.com	orugtuapnz.yi.org
qeqfsvxousx.1dumb.com	fzddikiyq.dynserv.com	ospknhemqt.yi.org
rjjuyi.1dumb.com	jdjsloy.dynserv.com	rdjqleu.yi.org
scdebvwcb.1dumb.com	jrscqsshxs.dynserv.com	tapdcm.yi.org
vfpqyv.1dumb.com	lslpcl.dynserv.com	yeaigapqs.yi.org
wbghid.1dumb.com	mtuixfkwd.dynserv.com	znvibonyf.yi.org
yutunrz.1dumb.com	mzpdswun.dynserv.com	
aazuxmmqqkq.3-a.net	ojcdsjl.dynserv.com	
amjcu.3-a.net	ooyvsk.dynserv.com	
cnntzas.3-a.net	pvxkideqlen.dynserv.com	
eniaaknrb.3-a.net	rzstdrbnzs.dynserv.com	
gxjitrjifgp.3-a.net	swywlq.dynserv.com	
ihhyzby.3-a.net	uhqoyjlu.dynserv.com	
imtoey.3-a.net	xfbdspu.dynserv.com	
ksfvgrf.3-a.net	aflnlpko.hn.org	
kyfabyzf.3-a.net	aragwzysxsj.hn.org	
mcduii.3-a.net	eqnjjsw.hn.org	
mlxvdl.3-a.net	firradbqzku.hn.org	
neytteybbo.3-a.net	gypzmaudtlv.hn.org	
qstffsupgu.3-a.net	ichyig.hn.org	
ryhszzinxss.3-a.net	ipurfbqpsdj.hn.org	
bdtjkfl.afraid.org	nttstzi.hn.org	
bhlnklify.afraid.org	nttstziinpa.hn.org	
ipbjty.afraid.org	tsyunetwmi.hn.org	
jquevnl.afraid.org	xatzjf.hn.org	

About Damballa, Inc.

Damballa protects businesses from targeted attacks used for organized, online crime. Our unique, global approach rapidly isolates the command-and-control needed to launch multi-network attacks. These signatureless solutions improve security both inside and outside the network perimeter, to stop threats other technologies miss and restore control to legitimate owners. Damballa identifies the severity and intent of targeted attacks such as BotArmies, even when malware can't be detected. These products and services provide a critical window for orderly remediation, and integrate easily into existing infrastructure without requiring additional headcount or complexity. Damballa is privately held, and is headquartered in Atlanta, Georgia.

Copyright © 2008, Damballa, Inc. All rights reserved worldwide.

This page contains the most current trademarks for Damballa, Inc., which include Damballa, the Damballa logo, BotArmy and BotMaster. The absence of a name or logo on this page does not constitute a waiver of any and all intellectual property rights that Damballa, Inc. has established in any of its products, services, names, or logos. All other marks are the property of their respective owners in their corresponding jurisdictions, and are used here in an editorial context, without intent of infringement.