Analysis of the Kraken Botnet

Paul Royal

April 9, 2008

Purpose

This document provides a concise analysis of the Kraken botnet. In addition to detailing the technical specifics of the Kraken bot malware and its communication with the Command and Control (CnC), this report includes a brief set of instructions for confirming compromise of and remediating Kraken-compromised hosts.

1. Kraken

1.1 Overview

Kraken is a large botnet currently used for spamming; examples of the junk and/or fraud-inducing email it sends are included in Appendix A of this report.

The Kraken bot binary uses algorithmically generated domain names of Dynamic DNS (DDNS) providers Yi, DynDNS, Afraid, and DynServ (now defunct) to locate and communicate with the botnet's CnC. To initiate communication with the CnC, the malware instance will generate a string of between six and eleven characters and append it to one of the DDNS second level domains yi.org, dyndns.org, mooo.com, or dynserv.com to form a "candidate" CnC domain name (e.g., bdubefoeug.yi.org). Before generating domain names, the Kraken binary will attempt to connect to several hard-coded IP addresses on TCP port 25. Depending on whether this connection is successful, the Kraken binary will generate one of two different, disjoint sets domains. Lists of the domain names for each these sets are provided in Appendix B.

Upon successfully locating an active CnC the Kraken binary will communicate using both UDP port 447 and TCP port 447. Packet payloads are encrypted with what evidence suggests is a 64-bit key. TCP communication occurs less frequently than UDP communication and likely represents spamming instructions and/or a binary update. Following TCP communication, the Kraken-compromised host will initiate a spamming run.

Damballa currently has 53 distinct Kraken bot samples; a listing of these samples by their MD5 value is provided in Appendix C. These samples are available upon request to any information security professional at an accredited organization.

1.2 Remediation

Due to the low AntiVirus (AV) detection rates for the Kraken bot malware, a host with up-to-date AV software may report that no malware is present, even though it is compromised with Kraken. Given this problem and in conjunction with its release of Kraken-compromised IP addresses, Damballa has created a set of instructions detailing how to identify and remove Kraken bot malware from a compromised host.

Legal Disclaimer: Although every reasonable effort has been made to ensure the accuracy of these instructions, Damballa assumes no liability for damages incurred directly or indirectly as a result of their use.

1.2-1 Compromise Confirmation

Before proceeding with remediation, confirm that the host is compromised by running a packet sniffer (e.g., tcpdump, ethereal) and looking for the following network-level symptoms:

- DNS lookups to domains ending in yi.org, dyndns.org, mooo.com, or dynserv.com
- Outgoing TCP or UDP packets with destination port 447 (encrypted payload)

1.2-2 Remediation

Upon confirming that the host is still compromised with Kraken, it can be remediated by using a simple two step process, which consists of:

1. Identifying the process name and location of the Kraken bot malware on the host;
2. Terminating the Kraken process, deleting the Kraken bot malware and restarting the system.

For Step 1, note that the name of the Kraken malware process will be between one and eleven randomly generated alpha characters. Using Windows TaskManager, look for an out-of-place process name running on the host that matches this description. After identifying a candidate process name, confirm its identity by looking for an executable of the same name in the system32 directory (e.g., C:\WINDOWS\system32\). Kraken bot malware will have an image file icon; confirm that the target executable does before proceeding to Step 2.

For Step 2, remediate the host by doing the following:

1. Terminate the Kraken malware process. Using Windows TaskManager, right click on the target process and select “End Process”. The process name should disappear from the list in Windows TaskManager.
2. Delete the Kraken malware executable file. Enter the system32 directory containing the executable file, right click on the file, and select delete. If necessary, enter the Windows Recycle Bin and permanently delete the file.
3. Reboot the system.

After rebooting the host, confirm that it no longer exhibits the network-level symptoms described in Section 1.2-1. Remediation is complete.

Appendix A: Kraken Spam Examples

Subject: Only quality meds at the cheapest cost

Do you want to save your time and money?
At present you can get meds sitting at home
*Best-selling medical products
*Big variety
*The lowest price you have ever seen

http://www.vfraionec.com

Subject: US$ 999 bonus with every new signup! limited time only

Play this game for free right now and get $ 999 for free
The famous Las Vegas casino Sands has decided to launch a online casino. .
Grab your 500% Deposit Bonus now! Up to $10,000 for all new customers!

http://www.gamblinsonlinecasinoyg.com.cn

Subject: Best Collection & Sw|ss R0lex! Spring SALE

Hello.
Dear client we are happy to offer you most most popular watches by famous brands.
Now you have marvelous chane to buy watches by the cheapest cost.

* Low prices
* Big variety
* Worldwide shipping
* Perfect quality

http://luridutskiwis.com

Appendix B: Kraken CnC Domain Names

aafsyt.dyndns.org	fvivkenao.dyndns.org	jydgko.dyndns.org
aetqzvfzub.dyndns.org	fxhbaxmuakb.dyndns.org	kbhtmpyw.dyndns.org
aifuunhoomc.dyndns.org	gdqnofcwvim.dyndns.org	kczuuykc.dyndns.org
akuqejwvztx.dyndns.org	gfzcwpunx.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	gmqaeoeudhd.dyndns.org	kpjobheecz.dyndns.org
bdzxcl.dyndns.org	gmsaxtqrn.dyndns.org	kpzlenrn.dyndns.org
bezmabz.dyndns.org	gnkovlb.dyndns.org	krgdnikw.dyndns.org
bfhagswbf.dyndns.org	gqwxcgusq.dyndns.org	ksxqzyfsnif.dyndns.org
bjjdhgpby.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	hjviglrwd.dyndns.org	lfqbim.dyndns.org
bxlginh.dyndns.org	hmhauqssekw.dyndns.org	likkhxbl.dyndns.org
cczxqasliks.dyndns.org	hnkoso.dyndns.org	lkgdxl.dyndns.org
cipaxqmcgfz.dyndns.org	hpnitjssj.dyndns.org	lkhlzwvb.dyndns.org
cvvhgffch.dyndns.org	hrlgrh.dyndns.org	llkzijizw.dyndns.org
cyytqnxz.dyndns.org	htlosdk.dyndns.org	llmqjmx.dyndns.org
dakxslvxy.dyndns.org	huslbscekh.dyndns.org	lquely.dyndns.org
danssxjpgqh.dyndns.org	ibfxdlyzdm.dyndns.org	lraxjgzdggv.dyndns.org
dftinvlu.dyndns.org	iefavv.dyndns.org	lslxgkyn.dyndns.org
djealpwfh.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
dztxvpt.dyndns.org	ipgcyhufwqw.dyndns.org	mqiuao.dyndns.org
echxfsqy.dyndns.org	ivybjwxblai.dyndns.org	mqwjwoyuyf.dyndns.org
ehlskzmg.dyndns.org	izucjnv.dyndns.org	mvcjpjbymby.dyndns.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
esbdelcjwmx.dyndns.org	jjmiak.dyndns.org	nbhbzxjvmyg.dyndns.org
esycuzpqk.dyndns.org	jnhmue.dyndns.org	nbtqhzhloxw.dyndns.org
etrzubdna.dyndns.org	jnwxvchqcr.dyndns.org	ndbpxddj.dyndns.org
ezynefc.dyndns.org	jolpfzruup.dyndns.org	ndgmklb.dyndns.org
fdsnwcrtjnh.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
pwoyexstwv.dyndns.org	vzzbeamwie.dyndns.org	ycofnn.dyndns.org
pwrbxafiyhf.dyndns.org	wabuku.dyndns.org	atgoycu.dyndns.org
qsxhvbwuf.dyndns.org	wbmmpbjf.dyndns.org	ckwklamspio.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	gzhhlhb.dynserv.com
rjlymb.dyndns.org	wvqzgyfkasp.dyndns.org	hsbyswcyqgk.dynserv.com
rjukvyfrkw.dyndns.org	wwkgpfiz.dyndns.org	ahlpxy.dynserv.com
rlgybcjevjx.dyndns.org	xawpaoq.dyndns.org	adrxokqn.dynserv.com
rlxnpfwpys.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	xckzkp.dynserv.com
rsawfg.dyndns.org	xorjoet.dyndns.org	vtdddxys.dynserv.com
rsxhoojs.dyndns.org	xoweqtscuy.dyndns.org	ebksscgdcc.dynserv.com
rxsqqcss.dyndns.org	xwnlbfcppmv.dyndns.org	vddlysri.dynserv.com
sfhksfw.dyndns.org	yappjfassl.dyndns.org	uvbvdmodc.dynserv.com
sjxhzwvtj.dyndns.org	ybilwkaz.dyndns.org	anrgxq.dynserv.com
smpyfxs.dyndns.org	ymcotzrr.dyndns.org	nvhjzbpl.dynserv.com
smwytfqyde.dyndns.org	ymunqnlcw.dyndns.org	nvnxznygos.dynserv.com
spycoqeywmk.dyndns.org	ysyzetd.dyndns.org	hshfmrobfjr.dynserv.com
sqnkiz.dyndns.org	yxjanpevse.dyndns.org	jlpswkv.dynserv.com
sransxyzp.dyndns.org	zjcquwl.dyndns.org	tkoappwny.dynserv.com
stxzbnnll.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	zuvzbng.dyndns.org	oaioaojp.dynserv.com
thgpkqh.dyndns.org	adrcgmzrm.dyndns.org	ocjvlbqs.dynserv.com
tjptbtrbgke.dyndns.org	lfiavsbyntu.dyndns.org	xqgonbfwye.dynserv.com
tkhqti.dyndns.org	iskqszufrft.dyndns.org	ocqkgmoa.dynserv.com
tlkrqxbtj.dyndns.org	mszbnhwzhvv.dyndns.org	odaqaqkttm.dynserv.com
tnifpmeh.dyndns.org	xnzkdos.dyndns.org	uokvzojl.dynserv.com
toafns.dyndns.org	vsdzee.dyndns.org	zpuxycznd.dynserv.com
toauarcnav.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	sjkjtfajx.dynserv.com	wmoutza.dynserv.com
jmyyptoo.dynserv.com	pxihdssdnvb.dynserv.com	hnmgivqndrk.dynserv.com
eihasibowm.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	yknskhnrsj.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	rzfwowcrt.dynserv.com	kuhzahg.dynserv.com
ttykgsvq.dynserv.com	qljpnkbjij.dynserv.com	xtuuqvgfbi.dynserv.com
osvfjswcnn.dynserv.com	qmnnxv.dynserv.com	dzsjniwffrx.dynserv.com
xoskcy.dynserv.com	ezfllrfh.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	qrcuota.dynserv.com	yoriulioeo.dynserv.com
hovdworcxd.dynserv.com	rokjemchbd.dynserv.com	dwlkloufb.dynserv.com
zyaquzholfi.dynserv.com	ykvzjuq.dynserv.com	wirmkbkikk.dynserv.com
yivdetzgvs.dynserv.com	xmbryakrity.dynserv.com	iqozgozb.dynserv.com
eoiovsv.dynserv.com	ewahbzgw.dynserv.com	ypscls.dynserv.com
pdduitmqhzj.dynserv.com	kfqbqbx.dynserv.com	lbkhtebgit.dynserv.com
pdfaswmn.dynserv.com	qtoftdrsbx.dynserv.com	dsbhsflxfc.dynserv.com
tjgpkyvtob.dynserv.com	xttjdfr.dynserv.com	drdioqdjho.dynserv.com
pepntatkq.dynserv.com	rnfmtpiet.dynserv.com	dpjrhrvxy.dynserv.com
frcgwebfwmh.dynserv.com	qxsaxoacg.dynserv.com	doxokpbliuz.dynserv.com
titstvez.dynserv.com	qyjceavgdsq.dynserv.com	dldhzpphgwa.dynserv.com
jqwnnincqwz.dynserv.com	rbltobttor.dynserv.com	xhhifkm.dynserv.com
pspypf.dynserv.com	gugjymmo.dynserv.com	irurmiseo.dynserv.com
uaqjtycx.dynserv.com	rcrwuqtcmwf.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	ljyjldhdshf.dynserv.com
stingvr.dynserv.com	wqwttk.dynserv.com	diyermz.dynserv.com
ilrmjjuz.dynserv.com	cfcsndquwjc.dynserv.com	diqici.dynserv.com
cwrrdxye.dynserv.com	rijvir.dynserv.com	itytizvqdjf.dynserv.com
dljemwae.dynserv.com	kmubffne.dynserv.com	dhievgx.dynserv.com
yisqdvqg.dynserv.com	rjevqixpsjs.dynserv.com	dgbxzfg.dynserv.com
jyyllmnemvx.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
jzdwbfr.dynserv.com	rluxdhubir.dynserv.com	ysiefvjp.dynserv.com

ptzjyxymqof.dynserv.com	endfyjc.dynserv.com	llzvkwmexh.dynserv.com
putphxcrz.dynserv.com	ymikwrqqrrg.dynserv.com	xgyllfmhtyv.dynserv.com
hnukbxx.dynserv.com	vrybipcapn.dynserv.com	yabpedfs.mooo.com
lotyzvchnn.dynserv.com	mxzszjjtac.dynserv.com	jixiqvsguut.mooo.com
hyoiwjx.dynserv.com	xdbxaaf.dynserv.com	jlbkzpjgn.mooo.com
vvjfsoj.dynserv.com	gestlmvmjqq.dynserv.com	jlqpeujbjbp.mooo.com
ytgvyywx.dynserv.com	bafirop.dynserv.com	yauhxoxb.mooo.com
hctrgy.dynserv.com	axxubqahlae.dynserv.com	ybgcei.mooo.com
ytkvvuknpt.dynserv.com	vcpcnqi.dynserv.com	jqbcxu.mooo.com
xoogblws.dynserv.com	urgfiluop.dynserv.com	jqkjkz.mooo.com
dbtteg.dynserv.com	hrwxno.dynserv.com	ydedcqpdble.mooo.com
hawkhllxek.dynserv.com	vrirjfuzfrx.dynserv.com	yhzddltofq.mooo.com
dbsioal.dynserv.com	awzzsd.dynserv.com	jzzyjaiede.mooo.com
ytszykjvn.dynserv.com	gejqvonji.dynserv.com	kbrzkkg.mooo.com
gvgqpueeq.dynserv.com	nghhezqyrfy.dynserv.com	ymbepny.mooo.com
iyiznt.dynserv.com	nhalhad.dynserv.com	khufndoqpz.mooo.com
wbgoeu.dynserv.com	atxkjyarv.dynserv.com	kiingoc.mooo.com
lwrjmu.dynserv.com	zkuppsly.dynserv.com	klmtord.mooo.com
gmkxtm.dynserv.com	aqixuwkwudv.dynserv.com	ymmsztgnb.mooo.com
lygjvassxij.dynserv.com	xpmsjptzw.dynserv.com	krpruobbtcn.mooo.com
wbfwwrrjo.dynserv.com	xydjuwfft.dynserv.com	ynfqicvyyqr.mooo.com
lytyicrge.dynserv.com	ammnifbseja.dynserv.com	kunjbkpp.mooo.com
cyiiejrr.dynserv.com	gbtpyjs.dynserv.com	yohhiu.mooo.com
lzvuyqoiom.dynserv.com	vqqcfgm.dynserv.com	lawzaa.mooo.com
yueire.dynserv.com	hnkypvj.mooo.com	lfreyzkcr.mooo.com
makpvgrpm.dynserv.com	hpapprvyh.mooo.com	lfwftbtdgjh.mooo.com
cpsmqekpse.dynserv.com	humbjatp.mooo.com	lfwjkwa.mooo.com
gkenyoabmg.dynserv.com	hwrmjis.mooo.com	lgqlhy.mooo.com
iziavxznxp.dynserv.com	hyffjoxbrq.mooo.com	lkuekdxbofy.mooo.com
ciliejchzm.dynserv.com	hzxghrpsxv.mooo.com	lmfviji.mooo.com
gjrscjz.dynserv.com	icixemu.mooo.com	lnbyesrxp.mooo.com
cditpjxmgdy.dynserv.com	icspdh.mooo.com	loyalneu.mooo.com
izlwodgff.dynserv.com	idzhbmy.mooo.com	lrcxtd.mooo.com
aqtxloupefy.dynserv.com	xpnbsq.mooo.com	lszxzxnw.mooo.com
gzwqowjpk.dynserv.com	igoygdf.mooo.com	lugzmfs.mooo.com
jbnsnx.dynserv.com	xqkpcbort.mooo.com	lunajs.mooo.com
giyscw.dynserv.com	xrbxpl.mooo.com	lvdnbndowai.mooo.com
vyrizkpu.dynserv.com	ilcbcbsxdk.mooo.com	lwsqwnzom.mooo.com
ghmelx.dynserv.com	immanrynlap.mooo.com	yuwzsixzuh.mooo.com
mqctckevqpj.dynserv.com	inlwntrol.mooo.com	mcotackq.mooo.com
brrpirqpixi.dynserv.com	inxxkp.mooo.com	medhtzj.mooo.com
vxfbmdnlph.dynserv.com	ivhhct.mooo.com	ywlacvk.mooo.com
bpjciclpp.dynserv.com	ivodajlpp.mooo.com	mhqbszalsp.mooo.com
xmlhbwd.dynserv.com	xuxsczv.mooo.com	mhxdfu.mooo.com
bosxrhq.dynserv.com	iwxjwww.mooo.com	minkoq.mooo.com
mvxsyyrs.dynserv.com	ixoynk.mooo.com	momktjnclgk.mooo.com
mwadqdc.dynserv.com	iybexlxx.mooo.com	yyxrelchaix.mooo.com
bmycoj.dynserv.com	xvczzlgflrn.mooo.com	zcxutl.mooo.com

mwpqsccj.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	agdwgsptbxo.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
nwyqyq.mooo.com	ftytgfehixd.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	ryvenskbkk.mooo.com	vsidyaikx.mooo.com
ouancdi.mooo.com	rzxoiewf.mooo.com	bfsznvjrsvt.mooo.com
patwcfb.mooo.com	safbvwgortr.mooo.com	bhimcgfl.mooo.com
pazduvpgg.mooo.com	sapgvql.mooo.com	bissgm.mooo.com
zyjdvgihz.mooo.com	sbbyvnpms.mooo.com	bjisvur.mooo.com
pfyxqhanw.mooo.com	scttfzou.mooo.com	boooxl.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	sunncpnswo.mooo.com	cfprocus.mooo.com
ptxmmkgr.mooo.com	swsmyvc.mooo.com	chqycawqy.mooo.com
pwlpzrylrun.mooo.com	sxoogybzgjv.mooo.com	ckvzxmc.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
qmqbnwyzewa.mooo.com	cmviueadnal.mooo.com	dablid.mooo.com
qqkxdhw.mooo.com	iwstwvw.mooo.com	drpwkpipsp.mooo.com
sfsocnwdnw.mooo.com	trppywlyuf.mooo.com	smgojbhuyw.mooo.com
qtdmcra.mooo.com	tsbvewputv.mooo.com	ebdqxgnm.mooo.com
qteaali.mooo.com	tuoswxeoclw.mooo.com	efwmtpedgyy.mooo.com
qtkbjdx.mooo.com	tzvhyc.mooo.com	emdunxqvvjf.mooo.com
quqozf.mooo.com	ufdwpgvj.mooo.com	eoxjsnvzuh.mooo.com
rckyibrjmrw.mooo.com	ykrzcragnnu.mooo.com	esbwimya.mooo.com
revvpzuuv.mooo.com	unjighufx.mooo.com	zztsqfzsbdb.mooo.com

tjetqly.mooo.com	uqmwgucn.mooo.com	evnmcjcbj.mooo.com
rjxnpjf.mooo.com	uvsbzwy.mooo.com	evyharj.mooo.com
rhpstjtlwdm.mooo.com	uzxnneqh.mooo.com	fhavrcvziql.mooo.com
znkhrtojwx.mooo.com	vedrtwtyw.mooo.com	fhfaronxx.mooo.com
wyyozskwecl.mooo.com	niyqqfxygly.yi.org	byrubffha.yi.org
wzmdmzfht.mooo.com	avlgaoar.yi.org	calovhzpsv.yi.org
fpeirgwhxjs.mooo.com	avsyzltsjqp.yi.org	jhafczshwfv.yi.org
xapjjfglotq.mooo.com	nfluntl.yi.org	mhctdivn.yi.org
ftotupatsxp.mooo.com	nflhsmjjuh.yi.org	cdcbqqtzluc.yi.org
fuodqqxsdz.mooo.com	axpehmxd.yi.org	mfaovpr.yi.org
fvcpbtsk.mooo.com	zgvxgm.yi.org	cdocrguwf.yi.org
fwisyzp.mooo.com	zfmheud.yi.org	cehxrq.yi.org
fxsigsvhyjz.mooo.com	pcajqcaof.yi.org	ceuswc.yi.org
fybjazu.mooo.com	xtlczgyi.yi.org	xpewycmkiu.yi.org
gacpcwgwd.mooo.com	bbblhihks.yi.org	cfbpsdxtijt.yi.org
gbtdmaomtr.mooo.com	gxoebjd.yi.org	xlfstaxlrui.yi.org
gbviecjbs.mooo.com	bbnmuuscwm.yi.org	chdgoxpfs.yi.org
xcvbmaxkrt.mooo.com	bdubefoeug.yi.org	jftkte.yi.org
xfkixgpjlq.mooo.com	mxybuuvfjzi.yi.org	chznlw.yi.org
gjewqe.mooo.com	ilwclwblahl.yi.org	yvmhvap.yi.org
xhlmrrbs.mooo.com	vutpaq.yi.org	itifvo.yi.org
gotlokmbwhh.mooo.com	jktktuoow.yi.org	wyudom.yi.org
gqtmrgtbkak.mooo.com	zctyzkvlosi.yi.org	hbqfqs.yi.org
guwyaqagyz.mooo.com	mwqgwuqu.yi.org	cngavndedml.yi.org
gwfmgh.mooo.com	fwaxdmjesfh.yi.org	cnrrizbhhm.yi.org
hadgfilg.mooo.com	bhrxmwhjs.yi.org	coypkaecyz.yi.org
hfltemaw.mooo.com	bhtioi.yi.org	cpiqlfej.yi.org
hinqarp.mooo.com	bibgwzvuy.yi.org	yuvuhsw.yi.org
hjbqfyg.mooo.com	iklnafi.yi.org	csoyrmxitit.yi.org
hjntjfyeqe.mooo.com	bjdpms.yi.org	xvyfxxcyym.yi.org
xnklfsjst.mooo.com	xcloyln.yi.org	cvkeykvgas.yi.org
hmhxnupkc.mooo.com	vwernpcpt.yi.org	hzlicyml.yi.org
hmruxtb.mooo.com	mwgoefg.yi.org	jcoklydzugy.yi.org
hmsaqrfsft.mooo.com	gwyziux.yi.org	cybckpcx.yi.org
nqpsra.yi.org	boabspnkjt.yi.org	lzpmyedjxgi.yi.org
vpjifkambi.yi.org	iexyznn.yi.org	waxmtzkqblh.yi.org
iocfyscy.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	lwfjtjabdsb.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	mqnmjv.yi.org	llddjb.yi.org
andcuaylu.yi.org	cdggua.yi.org	lkxdrhqml.yi.org
imyonl.yi.org	jjtvmoptq.yi.org	dgfboc.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	snzftifdwr.yi.org	okoovh.yi.org
dmnffduljev.yi.org	psrjan.yi.org	hgswylecgom.yi.org
wibausx.yi.org	wmvrlpvpqxu.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	pkkkepdgy.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	uvjvvqpjl.yi.org
laebdbptt.yi.org	tdtccdfb.yi.org	ezmpfzfglt.yi.org
dvwyrgkjr.yi.org	iuiqjzqrlwx.yi.org	uwsyasugjdp.yi.org
dwfbta.yi.org	gviailawmc.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	knzvnunfpf.yi.org	nteribmo.yi.org
rxgczwbyhvq.yi.org	pgjllls.yi.org	tqrvhfsdlup.yi.org
dzbzgittmwd.yi.org	pdmtvipa.yi.org	nszxnvzw.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	fhbwqikf.yi.org
sbsuzkh.yi.org	zwhutmqv.yi.org	vnvfrjxtpq.yi.org
qgvwxzw.yi.org	gdrlhg.yi.org	vouwbqfi.yi.org
ktggxfhmkfk.yi.org	iqubqksbudz.yi.org	
qgcytyogo.yi.org	klkkwdwzqco.yi.org	
sfbxsg.yi.org	tsjoiwyhmc.yi.org	
iypobnn.yi.org	klofmvcx.yi.org	
sglrundy.yi.org	osfnzylkv.yi.org	
kqgcvvv.yi.org	hqedhgimgz.yi.org	
ngbmfsbuql.yi.org	zswiqpmcsxw.yi.org	

sjriqtnzq.yi.org	etwyrs.yi.org	
sjwdfzvo.yi.org	opqhfeb.yi.org	
wmbmobl.yi.org	opjkkihbm.yi.org	
kpwyhgcii.yi.org	zrvpvlzyoky.yi.org	
ptntsmsg.yi.org	dstgrg.yi.org	
iyjofi.yi.org	iptwga.yi.org	

Appendix C: Kraken Bot Malware Sample MD5s

10fd78f9681d66d2dd39816b5f7f6ea6
18d16a05155748d65bdb41145e98912f
210d237f108bfcb23d987d8fa2f3d1c6
23ff402c9df630d9bad31515edc21dae
266720e7e859e0720e52d8d266629f10
3f3a945c792ab722b155f3305b8581f4
421333c17cb43ff7e5f961f5f13e2911
4629d0f73a48df3ee3be4d152fdb85f6
483580b7b95be355de57b1ee940a889b
485cd52e44d3df1f499fddcebcf140b6
4abbfe22e4803a9e931417a9d88f787e
4b590486cf8c046658c64104472e397d
52f13701ae011d1b98092d07bcaad043
5639a80421a098c9ce089fd335c04f50
592523a88df3d043d61a14b11a79bd55
60838eeb3f8cd311de0faef80909632d
62587160387c9bac604b99e4074055b9
6b4a99574af6ae5d2be703e91a35a36c
6dc48be5a53570ea63c02f178ebc7bcd
6efe376e306aa63caf956a8a1e13a2d5
77cf14bf1d0d88e6e6b9a0b99f8490ed
790c57dbcfae6ce122aac830065e0320
7ecef2f126e66e7270afa7b803f715bc
84446abe47a16387bd1f890ec05c3b9b
88a94a282417ee2a8c17bc6ee3613de9
8d96002e1374351936da764f65708740
98194f186669fb13751408eb858f40aa
981b353926deea203a61d4873ef94ede
9e6e57eda3eb3ea0fcae81b349191944
a48832210b4a05a7c0196d0208e6b8cd
ac37b1045c51b1b86744970b75a8e350
afb4b7f8be2965687fce33f9d0a80338
b0e7ac28f0a899afa0fcdda5f1252675
b3c78f1e7e81c02eed092e6f813a06df
c05eb75e00d54a041a057934979fed6d
c51abb75de3f8f8c225dacfbe1c2c715
c5d9edfa62368f8e93065e6912fbde3c
c7b440803846e413c7b417b16046d6d1
c853373764d86b927472766bd622e1ee

cc16f5fdf705fe76f61588561f866c29
cc33d7d6a6d901ddaa72fdf18d6bfb7e
d4331f7d1bc564772dc55ff80b5286da
d4749ef1edaf4c58e323973430acb964
d527bf3602107be86909fcf986155f51
ddb00e36e919802f92a7a99c7f933ea3
e5f9da179ece84c0c7ec0b325cb9194f
e6dcca6961f79df9b63bf6c311cfd183
ee3a48d89399e3ad6b1576a28db4d30d
efa97074d07523e9aa8709e1c36b42fc
f2c34a56a33ee7a22e77a217f5c9e92b
f403a99808137c1b4b5319e4d63f6dcc
fb57076a1a523f7a214634f52f934e6b
ffc2e41d8e729c7b8622a8420767cfb5

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.