Chapter 1

[8] 3ab45z.exe – PWS:Win32/Zbot!GO

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
bdn						
ifnjcavyljzcelbafutijamfazg.ru	1	ifnjcavyljzcelbafutijamfazg.ru	0.999976	559	279	280
ayyhmrrceicmgybeliraifqwcrk.org	1	ayyhmrrceicmgybeliraifqwcrk.org	0.999993	559	279	280
uoqspvtuotpusfigypvyxmzir.ru	1	uoqspvtuotpusfigypvyxmzir.ru	1.000000	559	280	279
tteyzamuwfyjnkzqwoztlvdsc.net	1	tteyzamuwfyjnkzqwoztlvdsc.net	1.000000	558	279	279
cihaiusscyptceumzwkqcsksk.org	1	cihaiusscyptceumzwkqcsksk.org	0.999984	558	279	279
xcwcqfqxwtdihgyvozxkfhqwwg.info	1	xcwcqfqxwtdihgyvozxkfhqwwg.info	0.999988	558	279	279
hyzdxwtwxexwjndnbsjv.com	1	hyzdxwtwxexwjndnbsjv.com	0.999973	558	280	278
lleaxypmvlbljcqzphqsgugzt.info	1	lleaxypmvlbljcqzphqsgugzt.info	0.999861	557	278	279
tltkbmciylqscyhfqmvtgqkeq.net	1	tltkbmciylqscyhfqmvtgqkeq.net	0.999999	557	279	278
dyzvkwktlnzpaihugewtstzd.net	1	dyzvkwktlnzpaihugewtstzd.net	0.999999	557	278	279

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	3460/3460	cihaiusscyptceumzwkqcsksk.org uoqspvtuotpusfigypvyxmzir.ru xcwcqfqxwtdihgyvozxkfhqwwg.info tteyzamuwfyjnkzqwoztlvdsc.net	0.998734	731100	365694	365406
0.50	50/50	ayyhmrrceicmgybeliraifqwcrk.org ifnjcavyljzcelbafutijamfazg.ru tceutceqdqukrgitwgjvyhxsojbeem.org lleaxypmvlbljcqzphqsgugzt.info	0.999990	27652	13800	13852
0.20	2/4	ovxswpduosooozuwumeacqzxmz.info mx2.h2.net.au mx4.h2.net.au mx3.h2.net.au	0.250005	484	386	98
0.30	57/57	avceuhcyhowgvogqlbcmcqcx.ru wmbmhtktcjrbyzkxorwpsotzd.org dqtkzzlmvxauhqxgpztvsrcfaded.com ydvowcfmonzlqxkznbdusxsll.net	0.999981	171	114	57
0.10	1/1	hmraeqijkjzluxpxrclfyeqs.info	0.999997	450	401	49

Dynamic DNS providers:

dn		top10m	nosfx	app	ok	nx	nx/app
Four examples	unique	mean	mean	sum	sum	sum	mean
h2.net.au mx2.h2.net.au mx4.h2.net.au mx3.h2.net.au mx1.h2.net.au	5	NaN	0.000005	20	16	4	0.21

Chapter 2

[22] oleprn.dll – Trojan:Win32/Bulta!rfn

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	examples	nosfx mean	app sum	ok sum	nx sum
147.in-addr.arpa	1	216.83.32.147.in-addr.arpa	0.000001	681	681	0
yahoodns.net	9	mta5.am0.yahoodns.net mta7.am0.yahoodns.net mta6.am0.yahoodns.net mx2.sbcglobal.am0.yahoodns.net	0.000097	482	482	0
psmtp.com	34	automatedconcepts.com.s8a1.psmtp.com kaplan.edu.s8a1.psmtp.com Friedbergjcc.org.s8a1.psmtp.com dwkcb.com.s6a1.psmtp.com	0.000122	98	98	0
pphosted.com	16	mxa-0015db01.gslb.pphosted.com mxa-000f3001.gslb.pphosted.com mxa-0015b201.gslb.pphosted.com mxb-00123c01.gslb.pphosted.com	0.000005	60	60	0
GOOGLE.COM	3	ASPMX.L.GOOGLE.COM ALT1.ASPMX.L.GOOGLE.COM ALT2.ASPMX.L.GOOGLE.COM	0.000007	56	56	0
ctmail.com	1	p.nsm.ctmail.com	0.000006	34	34	0
ass-concerts.de	2	ass-concerts.de mail.ass-concerts.de	0.000076	32	32	0
vmb-1.com	2	vmb-1.com mail.vmb-1.com	0.000016	32	32	0
fincomplex.ru	2	fincomplex.ru relay.fincomplex.ru	0.000190	32	32	0
lidiasoselia.ru	2	lidiasoselia.ru mail.lidiasoselia.ru	0.000312	32	32	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	2/2	maxinomina.com mail.aa-mail.net	0.345744	6	3	3
0.30	1/1	ecomrider.com	0.000543	6	4	2

Chapter 3

[23] java.exe – TrojanDownloader:Win32/Dofoil!rfn

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
bdn						
xxciiqyefqyu.pw	1	xxciiqyefqyu.pw	0.999929	556	556	0
uyhgqunqkxnx.pw	1	uyhgqunqkxnx.pw	0.999978	549	527	0
rvqlfnedcldh.pw	1	rvqlfnedcldh.pw	0.999950	536	536	0
lpefukjwddgn.pw	1	lpefukjwddgn.pw	0.999750	532	532	0
fkmmvfeonnyh.pw	1	fkmmvfeonnyh.pw	0.999362	506	498	0
hhmgferksnfb.pw	1	hhmgferksnfb.pw	0.999827	499	414	85
llbyviyiqrkt.pw	1	llbyviyiqrkt.pw	0.999897	480	393	87
vjbrgpofghto.pw	1	vjbrgpofghto.pw	0.999862	460	375	85
ugsudtvxrypq.pw	1	ugsudtvxrypq.pw	0.999963	458	372	86
yyffsscwgolo.pw	1	yyffsscwgolo.pw	0.999934	454	366	88

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	982/982	tshouebcgjxq.pw mjhuduxhxuec.pw ggmluudorjno.pw vvcwripkvigi.pw	0.986919	412523	206793	205730
0.15	8/8	nqtllehiydgg.pw yyffsscwgolo.pw llbyviyiqrkt.pw ugsudtvxrypq.pw	0.999920	3696	3008	688

Chapter 4

[9] salesforce_ssl_cert.zip – PWS:Win32/Zbot

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok
bdn	num	examples	mean	sum	sum
yahoodns.net	3	mta6.am0.yahoodns.net mta7.am0.yahoodns.net mta5.am0.yahoodns.net	0.000032	19	19
lryhvkcsotlvhktjffuaioft.com	2	lryhvkcsotlvhktjffuaioft.com www.lryhvkcsotlvhktjffuaioft.com	0.999985	14	9
mbkveyukzxzxlbbmmzcmonxkabu.com	2	mbkveyukzxzxlbbmmzcmonxkabu.com www.mbkveyukzxzxlbbmmzcmonxkabu.com	0.999999	14	9
lthnvbepjvworeawsvoozeagq.com	2	lthnvbepjvworeawsvoozeagq.com www.lthnvbepjvworeawsvoozeagq.com	0.999962	14	9
xqavknbthqjvnvxsuojnrsc.org	1	xqavknbthqjvnvxsuojnrsc.org	0.999996	13	7
adedtppnnfmztussktlnbknkn.org	1	adedtppnnfmztussktlnbknkn.org	0.999925	12	6
ozqccpobpbfycarjvyhqcdptxk.biz	1	ozqccpobpbfycarjvyhqcdptxk.biz	0.999995	12	6
pbezllztcnjtqeuhovtiz.biz	1	pbezllztcnjtqeuhovtiz.biz	1.000000	12	6
payypdmhxcxxvgvsojdqs.com	1	payypdmhxcxxvgvsojdqs.com	0.999994	12	6
paupjzifvctqkemtku.ru	1	paupjzifvctqkemtku.ru	0.999977	12	6

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	1840/1840	fqdqceidwktljhemvxfqvggmgi.com pgizvqgeuauugkobcmusqogyqw.com gitcadqlfiprzzpfairvolnrc.biz hamncqugmkroncavskubmydqci.org	0.999876	14617	7309	7308
0.40	37/37	zdcqlfilnheambajvgorskkfl.net kfmrcleizdpnnbwcdaeaqotsojro.com zdsinjnkjzpmvdhrovytrs.com gugquwcumizhgyibbaqobajfvolbh.info	0.999978	444	259	185
0.30	11/11	xnjlytyxlhfypgexlt.net ughiztxzpzxookjjzojtvosl.com ltcswrowcthqmmnwodgergtolz.biz hucjrxbawcqwgapzuwwsrcwwglb.net	0.999984	132	88	44
0.20	25/25	rwovvgkrvgvmjrlzhtzwdts.com eaprcgudqvgscnfpinckvlwo.org teypztkciibkfkrluwzpgxbrc.net gqljbitozducautxogegmizqoqc.info	0.999988	148	111	37
0.05	18/18	hiciqglzaqwopnzdmtkdro.com nrdiqotuoxcbaxokrfqcilcal.info bepyxbamjlvlzcabuuwnjkbmcuztt.net towohjnpxozxqwvbyxgayvc.info	0.999981	216	198	18
0.15	5/5	uosksganzdxciftsroukwofip.com woxconfedrktwbeukzuktai.biz hybytqwscguvowbbgwgxijdq.com bjvinbegehaukxdsmfzpeq.com	0.999248	60	50	10

Chapter 5

[24] data.pif – Worm:Win32/Netsky

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
bdn						
zzz.org	2	zzz.org aaa.zzz.org	0.114680	370251	370239	0
ukw	22	b x 9 7	0.000000	325114	162584	162510
49.5	1	49.5	0.000000	124858	62439	62416
18.5	1	18.5	0.000000	124823	62415	62408
51.5	1	51.5	0.000000	124814	62410	62400
yahoodns.net	5	mx-apac.mail.gm0.yahoodns.net mta6.am0.yahoodns.net mta7.am0.yahoodns.net mta5.am0.yahoodns.net	0.000110	122382	122382	0
56.5	1	56.5	0.000000	93631	46821	46807
47.5	1	47.5	0.000000	93605	46807	46797
lacita.com	1	zinfandel.lacita.com	0.005017	92602	92601	0
kamagrakaufen.eu	1	kamagrakaufen.eu	0.000130	92578	92569	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	108/129	49.5 18.5 51.5 56.5	0.002833	2701570	1351135	1350330

Dynamic DNS providers:

dn			top10m	nosfx	app	ok	nx	nx/app
	Four examples	unique	mean	mean	sum	sum	sum	mean
ukw	b x 9 7	22	NaN	0.000000	325114	162584	162510	0.45
ucla.edu	cougar.noc.ucla.edu mx.smtp.ucla.edu mx-ucb2.smtp.ucla.edu mx-ucb1.smtp.ucla.edu	9	7380.0	0.000261	108894	62059	46827	0.05

Chapter 6

[10] FzPfH6.exe – PWS:Win32/Zbot!GO

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
bdn						
ayvcfcieulpxxoqgjrobojgafmc.biz	1	ayvcfcieulpxxoqgjrobojgafmc.biz	1.000000	428	218	210
ymjvcnrojthicixhgqdakrv.ru	1	ymjvcnrojthicixhgqdakrv.ru	0.999997	425	219	206
uylhmugfxdayzbqibhpbivkvsk.com	1	uylhmugfxdayzbqibhpbivkvsk.com	0.999997	424	217	207
gabozapbkbspbvwdlrdqfyam.org	1	gabozapbkbspbvwdlrdqfyam.org	0.999996	424	216	208
vghheaudpnjbnjhdhenrxzdba.ru	1	vghheaudpnjbnjhdhenrxzdba.ru	0.999996	423	216	207
qollfijdpvhdyuwxwkljzqw.org	1	qollfijdpvhdyuwxwkljzqw.org	0.999984	423	217	206
djcuqkuodcyhtijxjbtjnwomz.info	1	djcuqkuodcyhtijxjbtjnwomz.info	0.999990	422	216	206
wgtwcwsxszxljbuwsgmdaztkrxktg.info	1	wgtwcwsxszxljbuwsgmdaztkrxktg.info	0.999999	422	215	207
xojaydirsmzceqpnlroojobggyh.ru	1	xojaydirsmzceqpnlroojobggyh.ru	0.999986	422	217	205
rwfefqpkjopnhydxcbqguxoswd.com	1	rwfefqpkjopnhydxcbqguxoswd.com	0.999999	422	217	205

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	2193/2193	ayvcfcieulpxxoqgjrobojgafmc.biz gabozapbkbspbvwdlrdqfyam.org tkveiinvogqfqkbpjpjtghapj.info lvprjrceltaeuztnzzpwcpreuwwc.com	0.999775	710445	360048	350391
0.40	213/213	nrwsgikvxswoxbuuofmtgxwtkbcix.net qaevgmnwvkamaxwwdtkmzllrir.org odqxxsbieuxinwggujncyaudem.info mvngywoswknsotxnfonpvphqp.org	0.997593	1716	997	719
0.35	125/125	aiemvwdrsmnuovdrsuspkvxl.info aeluknbsorchuxspfbqpvzovhxg.info tkvotgejvmzlrztrcdxwytrdmaiws.biz hmhyhqtwcvsxkjvvugqkhvkvcirt.org	0.999980	1613	1008	605
0.30	162/162	laizhnvdejfonnbnzzugmnhuhixc.com cmrkbiauprhirpifgaxkambel.biz kvvoytukwaebexsgabqgbuaqulz.com nvugylrgcaurgivnftczhhqhpjj.biz	0.994537	1363	912	451
0.25	97/97	rwvcqcydaithofxzlhwsqchijz.org hezmbqemxgzltibljdqrsgqrwvwg.net kjtkvcbimbfelziniryxgemvifqcuc.net xknwszbaljwoqzpjhicmxw.com	0.999961	904	646	258
0.20	107/107	qwmcubqprizoirivhulnytpwkql.org pnjrsrofmtcttjvizxtgpzif.org bamrvkxoojwgzdlbdapreqmvuwt.info xwsobyaidmnfeudjffafqhucytk.ru	0.999959	763	582	181
0.05	7/7	ruclnbizvhdvwcmojijqkzxgm.info mvnbtroyttkjhiypbyfmztsmqoai.info wkdheprwfaptclhqkqdarsi.info pbvwcckjaqtcvcvofyemnzhbicux.org	0.999969	1791	1687	104
0.15	22/22	rcbvgrsxxytbitkprbaxgtgvc.net dwghmrukrfidyjzqgqcttwt.biz ytpftguqkduknhqhzlqopdprw.com swmnhetcxoushbawgjrhqcmjkbd.biz	0.999995	164	136	28
0.00	2/2	eqzlmnfushapbtofutpzhelws.com ypciaeifdmxhealvtjzrcgyvo.info	0.999996	576	563	13
0.10	6/6	eicibigmwsnbyxmgqrglnaqwsgbi.com njivrwkntodvsppforbafiwodjbaq.info smirgqtsgscknjnfknlzdy.ru degyojhxkrspnwgkfbarkxkeygu.biz	0.999962	46	40	6

Chapter 7

[12] WINAPI32.EXE – Trojan:Win32/Matsnu.R

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	examples	nosfx mean	app sum	ok sum	nx sum
requestpressure.com	1	requestpressure.com	0.995763	4774	2392	0
worddustballprocess.com	1	worddustballprocess.com	0.000087	4774	2392	0
trainingpursue.com	1	trainingpursue.com	0.629610	4774	2392	0
silverresolve.com	1	silverresolve.com	0.059112	4770	2390	0
substanceissue.com	1	substanceissue.com	0.103220	4758	2384	0
musclecuphospital.com	1	musclecuphospital.com	0.000302	2395	1198	1195
nailadaptbank.com	1	nailadaptbank.com	0.000139	2382	1191	1191
toweldependequipment.com	1	toweldependequipment.com	0.976628	2379	1190	1189
treeproducealarm.com	1	treeproducealarm.com	0.410529	1625	1508	0
taskshowerreaction.com	1	taskshowerreaction.com	0.034281	1210	1210	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

nx/app	bdn/dn num	dn examples	nosfx mean	app sum	ok sum	nx sum
0.45	68/68	musclecuphospital.com nailadaptbank.com toweldependequipment.com universitycrash.com	0.230321	23716	11859	11855
0.25	1/1	swimmingearnoil.com	0.041443	350	224	92
0.20	2/2	clickrepeatlaw.com starpaircarry.com	0.000411	228	125	55
0.10	1/1	assistanceisland.com	0.484227	238	121	25
0.00	1/1	closetmatterplane.com	0.000480	104	102	2

Chapter 8

[14] Mezzaluna calante.exe – Trojan-Banker.Win32.Tinba.hrd

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
bdn						
rkpiqcmmmbue.xyz	1	rkpiqcmmmbue.xyz	0.999975	2327	1264	1063
lvfxgvdofett.xyz	1	lvfxgvdofett.xyz	0.999833	2179	1128	1051
eviyrmxgxspl.xyz	1	eviyrmxgxspl.xyz	0.993917	2174	1119	1055
yxyyqbhgsjcp.xyz	1	yxyyqbhgsjcp.xyz	0.999954	2171	1116	1055
oodrrokoefls.xyz	1	oodrrokoefls.xyz	0.958422	2170	1116	1054
rqyxxxwwrrss.xyz	1	rqyxxxwwrrss.xyz	0.999962	2167	1119	1048
cjksfwrevcvm.xyz	1	cjksfwrevcvm.xyz	0.999942	2164	1112	1052
spfpujrbmmnv.xyz	1	spfpujrbmmnv.xyz	0.999893	2157	1100	1057
blxycnjtmygs.xyz	1	blxycnjtmygs.xyz	0.999598	2154	1104	1049
jkvvupijigwr.xyz	1	jkvvupijigwr.xyz	0.999957	2151	1096	1055

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	1001/1001	rkpiqcmmmbue.xyz rggderfidxhx.xyz jxihgmogkkgs.xyz nxhonrxwkbwh.xyz	0.976632	1239075	629655	609411

Chapter 9

[15] Postmodernism.exe – Trojan:Win32/Miuref.R

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	examples	nosfx mean	app sum	ok sum	nx sum
gatyhub.com	3	ww11.gatyhub.com gatyhub.com ww55.gatyhub.com	0.332648	21772	21640	0
qexyryl.com	1	qexyryl.com	1.000000	19155	19025	0
lymyxid.com	1	lymyxid.com	0.999806	19077	18946	0
vofygum.com	1	vofygum.com	0.999986	18928	18796	0
volyqat.com	1	volyqat.com	0.999991	18826	18694	0
lysytyr.com	1	lysytyr.com	0.999993	18814	18682	0
vonyjim.com	1	vonyjim.com	0.999981	18805	18673	0
galyvas.com	1	galyvas.com	0.999490	18803	18671	0
volybec.com	1	volybec.com	0.999820	18801	18669	0
purycap.com	1	purycap.com	0.976731	18800	18672	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	765/765	ganyhuh.com vofypuk.com qexyfel.com lyxyfar.com	0.994495	3629320	1836393	1792922
0.35	7/7	qekyqop.com vonyzuf.com qedyfyq.com gadyfuh.com	0.999936	42819	26334	16485
0.40	7/7	pufypiq.com vocymut.com gacyryw.com qegysoq.com	0.999905	38048	21563	16485
0.00	1/1	vocyzit.com	0.999978	16976	16561	308
0.50	1/1	wpad.lan	0.000000	24	11	13

Dynamic DNS providers:

dn Four examples	unique	top10m mean	nosfx mean	app sum	ok sum	nx sum	nx/app mean
winsrw.com 5.winsrw.com 1.winsrw.com 2.winsrw.com 3.winsrw.com	5	NaN	0.000006	10	9	1	0.09
web-counter.info 5.web-counter.info 1.web-counter.info 3.web-counter.info 2.web-counter.info	5	NaN	0.000008	9214	8369	845	0.09

Chapter 10

[27] ebb20174ee893c0754654668f3e837ff.exe – Trojan:Win32/Skeeyah.A!bit

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	
acn.name	1	cf0c69c2d0e0da8e900b06509bb
phicdn.net	1	cs9
pipeline-edge-prod-24-1300278808.us-west-2.elb.amazonaws.com	1	pipeline-edge-prod-24-1300278808.us-west-2.elb.
d12uj65dsn9ho1.cloudfront.net	1	d12uj65dsn9ho
d2k03kvdk5cku0.cloudfront.net	1	d2k03kvdk5cku
d1zkz3k4cclnv6.cloudfront.net	1	d1zkz3k4cclnv
d1sp2sgy246t7c.cloudfront.net	1	d1sp2sgy246t7
d2pp80vsjn2e6y.cloudfront.net	1	d2pp80vsjn2e6
d34chcsvb7ug62.cloudfront.net	1	d34chcsvb7ug6
d6wjo2hisqfy2.cloudfront.net	1	d6wjo2hisqfy

DNs having NX responses greater than 0, grouped by their NX/app ratio:

nx/app	bdn/dn num	dn examples	nosfx mean	app sum	ok sum	nx sum
0.45	1/1	wpad.lan	0.0	4	2	2

Chapter 11

[17] troyanproxy.exe – TrojanProxy:Win32/Bunitu.K

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	examples	nosfx mean	app sum	ok sum	nx sum
joinparty4more.xyz	3	ns8.joinparty4more.xyz ns0.joinparty4more.xyz ns1.joinparty4more.xyz	0.000022	72208	51826	20381
wdrimg.com	1	cdn.wdrimg.com	0.305926	359	359	0
solads.media	2	feed.solads.media cdn.feed.solads.media	0.000006	162	162	0
bnmla.com	1	soundwave.bnmla.com	0.006932	124	124	0
vip72.info	3	63678116.vip72.info 20058396.vip72.info 27180137.vip72.info	0.000624	68	34	0
adformdsp.net	2	server.adformdsp.net s1.adformdsp.net	0.009120	58	58	0
iias.eu	2	dev.iias.eu www.iias.eu	0.000093	58	58	0
webovernet.com	2	s1751.webovernet.com s751.webovernet.com	0.000004	54	54	0
letvertise.com	2	e0.letvertise.com cdn.letvertise.com	0.000003	52	52	0
eshopcomp.com	2	pstatic.eshopcomp.com istatic.eshopcomp.com	0.000067	50	50	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

nx/app	bdn/dn num	dn examples	nosfx mean	app sum	ok sum	nx sum
0.45	1/2	ns8.joinparty4more.xyz ns0.joinparty4more.xyz	0.00003	43063	22681	20381

Dynamic DNS providers:

dn			top10m	nosfx	app	ok	nx	nx/app
	Four examples	unique	mean	mean	sum	sum	sum	mean
whoer.net	bjjwf1446610.br.whoer.net dnfzm1447306.br.whoer.net odzhn1447289.br.whoer.net ovzfn1446717.br.whoer.net	16	366326.0	0.001025	159	128	31	0.378125
360.cn	s.so.360.cn reg.hao.360.cn qurl.f.360.cn s.360.cn	6	43304.0	0.000010	55	53	2	0.033333

Chapter 12

[1] 105.exe – TrojanDownloader:Win32/Obvod.M

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	
alacartebelini.com	4225	0.49921.pdl.alaca 220.42241.pdl.alaca 2.57099.pf.alaca 7.57099.pf.alaca
method.in	639	8f267a4596962193f2c0fa85ec902efb1647af54b85a690df6.f 8fda7859966a238ff23cf899ec6c2ce716bbad48b8a66b11f6.f 6.0.0.105.3467462492.1226377057.0.0.8f267a4596962193f2c0fa85ec902efb1647af54b85a690d 105.8f267a4596962193f2c0fa85ec902efb1647af54b85a690df6.
reduxmediagroup.com	1	ads.reduxmed
networkhm.com	1	ads.net
ajax.googleapis.com	1	ajax.go
fonts.googleapis.com	1	fonts.go
contentsiteonline.com	1	contents
iskullgames.com	1	www.isk
kenplay.com	1	www
pferdetoplist.de	1	www.pf

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok
	num	examples	mean	sum	sum
nx/app					
0.45	1/2	8f267a4596962193f2c0fa85ec902efb1647af54b85a690df6.fofi.method.in 8fda7859966a238ff23cf899ec6c2ce716bbad48b8a66b11f6.fofi.method.in	2.729039e-09	256	128
0.05	1/1	0.49921.pdl.alacartebelini.com	2.190402e-06	496	450
0.00	1/3	220.42241.pdl.alacartebelini.com 2.57099.pf.alacartebelini.com 7.57099.pf.alacartebelini.com	1.546001e-06	2680	2660

Dynamic DNS providers:

dn			top10
	Four examples	unique	mea
alacartebelini.com			
	0.49921.pdl.alacartebelini.com 220.42241.pdl.alacartebelini.com 2.57099.pf.alacartebelini.com 7.57099.pf.alacartebelini.com	4225	Na
method.in			
	8f267a4596962193f2c0fa85ec902efb1647af54b85a690df6.fofi.method.in 8fda7859966a238ff23cf899ec6c2ce716bbad48b8a66b11f6.fofi.method.in 6.0.0.105.3467462492.1226377057.0.0.8f267a4596962193f2c0fa85ec902efb1647af54b85a690df6.method.in 105.8f267a4596962193f2c0fa85ec902efb1647af54b85a690df6.ofi.method.in	639	Na

Chapter 13

[2] Htbot.exe – Backdoor:Win32/Htbot.B

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	examples	nosfx mean	app sum	ok sum	nx sum
adformdsp.net	2	server.adformdsp.net s1.adformdsp.net	0.009120	1538	1538	0
eshopcomp.com	5	pstatic.eshopcomp.com istatic.eshopcomp.com app.eshopcomp.com jsgnr.eshopcomp.com	0.000179	1392	1392	0
winnerical.info	3	zigad.winnerical.info mnh.winnerical.info direct_pop.winnerical.info	0.000006	1282	1282	0
tractions.biz	1	tractions.biz	0.000629	1120	1120	0
hokynar.eu	1	hokynar.eu	0.998213	1070	1070	0
onimp03.com	1	ads.onimp03.com	0.000007	956	956	0
ads.cc	1	beta.ads.cc	0.000002	772	772	0
sonux.cz	2	www.sonux.cz sonux.cz	0.000252	610	610	0
kingallshare.com	1	kingallshare.com	0.000029	554	554	0
wdgserv.com	1	weatherblink.wdgserv.com	0.672388	548	548	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

nx/app	bdn/dn num	dn examples	nosfx mean	app sum	ok sum	nx sum
0.45	17/32	locate.madserver.net superyou.zapto.org www.sonux.czhttp crimenc5wxi63f4r.onion	0.077478	1454	727	727

Dynamic DNS providers:

dn		top10m	nosfx	app	ok	nx	nx/app
Four examples	unique	mean	mean	sum	sum	sum	mean
whoer.net							
wpcek1432762.br.whoer.net	55	366326.0	0.000323	928	814	114	0.441818
uderg1431531.br.whoer.net							
sqzbm1432762.br.whoer.net							
bkuqr1428770.br.whoer.net							
facebook.com							
5-undefined.facebook.com	24	2.0	0.000084	1800	1779	21	0.112500
1-undefined.facebook.com							
6-undefined.facebook.com							
4-undefined.facebook.com							
dnsfor[0-9].(com—net—org)							
ns1.dnsfor7.com	18	NaN	0.000039	42	21	15	0.375000
ns1.dnsfor6.com							
ns1.dnsfor5.com							
ns1.dnsfor4.com							
twitter.com							
p.twitter.com	8	5.0	0.000114	795	775	20	0.056250
platform.twitter.com							
cdn.syndication.twitter.com							
syndication.twitter.com							

Chapter 14

[3] sample1.exe – Trojan:Win32/Necurs

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
bdn						
npkxghmoru.biz	1	npkxghmoru.biz	0.824690	38	38	0
vlteaqimk.pw	1	vlteaqimk.pw	0.998706	10	10	0
xkaihxporh.net	1	xkaihxporh.net	0.993293	9	7	2
geqxabrremsp.ms	1	geqxabrremsp.ms	0.998947	9	7	2
ojddowffjbxxv.so	1	ojddowffjbxxv.so	0.999956	9	7	2
amjvlrxcrdwcextb.mx	1	amjvlrxcrdwcextb.mx	0.999903	9	7	2
frnehhvncwhi.mu	1	frnehhvncwhi.mu	0.999946	9	7	2
qeyaixgptagjags.xxx	1	qeyaixgptagjags.xxx	0.998481	9	7	2
hoomiecqt.so	1	hoomiecqt.so	0.685286	9	7	2
wbuxdxkbgo.ru	1	wbuxdxkbgo.ru	0.999494	9	7	2

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	2259/2259	dhotfgpkotuxyeg.pro ngdqhxasuulekjqositot.ir gfeqavjhjb.kz emxxxkagjmfprj.nu	0.940148	4562	2281	2281
0.30	204/204	gvkqrrpjdadfpk.sx qaenaogkamr.bit wdetrxffhntb.nu mjwlchokhicl.org	0.951708	612	408	204
0.20	87/87	ukchrjlfpdp.cm wbuxdxkbgo.ru ojddowffjbxxv.so qeyaixgptagjags.xxx	0.938662	431	319	103
0.25	38/38	vcatvjamdfreaqdwg.jp ilannfddcymqroojwe.su jdhxomlooc.me kgkjphbxlcycdhfsycsy.ki	0.964370	266	190	76
0.15	15/15	koktdingohdelup.mn jqvkthaqhxpqsrqpksbg.sx bexldri.tv oqmtdkncaqolh.so	0.896746	90	74	15
0.10	4/4	mekicxiqxlmitp.im sflhmfmllkpspavg.in qwwgchsmllqkeitwdng.sx cudffmmqkojcrtlwrjbo.cc	0.999912	31	26	4
0.40	1/1	cixpyoskuds.mn	0.393134	5	3	2

Chapter 15

[4] yL0T.exe – PWS:Win32/Zbot!GO

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
bdn						
hulnfqtslpbwctkyxgqluoxkx.org	1	hulnfqtslpbwctkyxgqluoxkx.org	0.999895	286	144	142
zthubydughaxlbizttwsinmb.info	1	zthubydughaxlbizttwsinmb.info	0.999999	285	143	142
mrjxtorvtgydvcrslnqoghtus.info	1	mrjxtorvtgydvcrslnqoghtus.info	0.999992	285	143	142
mnlushyplndmkvjztskbrgtpru.biz	1	mnlushyplndmkvjztskbrgtpru.biz	0.999840	285	143	142
dmkjeybqeaorbigetswgegmda.org	1	dmkjeybqeaorbigetswgegmda.org	0.999997	285	143	142
qpflvxrrjbuknskwzvgwkyt.info	1	qpflvxrrjbuknskwzvgwkyt.info	0.999997	285	143	142
kzfayxscepzqkguyhsmfkbbmqgjf.info	1	kzfayxscepzqkguyhsmfkbbmqgjf.info	0.999996	285	143	142
onxuhatvheqgyxbydypzhbykz.org	1	onxuhatvheqgyxbydypzhbykz.org	0.999992	285	143	142
ijkhafitxkbkrwgqjztgtstayh.com	1	ijkhafitxkbkrwgqjztgtstayh.com	0.999990	285	143	142
dukzofukjfnrnypmwpyhlzh.org	1	dukzofukjfnrnypmwpyhlzh.org	0.999994	285	143	142

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	2637/2637	eijethacaxcgajrldmfu.info qamcytdfmhxifzdlnscsgucxg.net gmbaltckgqfuotodul.com ijnucdvmovlxfafmtslga.ru	0.998983	465782	232916	232866
0.30	35/35	scvbmtcqsonaplndhazd.com pjplifypaqdaljpnzpvwkjnbfa.com xgytveqvgjrnfyormvifvkzthm.com byljmqczhdqvsxfybeizzcp.com	0.999964	5905	3923	1982
0.40	1/1	qorofmjnvbapzvkguojauzsoaqk.org	0.999993	174	100	74
0.35	1/1	xpvxckjvcydmdyypeqmjoqttt.com	0.999997	168	109	59
0.10	1/1	dbmknpruovaicqcueywcukvkpjv.info	0.999995	230	201	29
0.20	2/2	obyhpvsuxkataqjlordfeh.ru dhapbcrgjntouctwbyhxeiiz.ru	0.999998	8	6	2

Chapter 16

[5] Setup.exe – Trojan:Win32/Tiggre!rfn

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok
	num	examples	mean	sum	sum
bdn					
forcedsharetraktor.live	1	forcedsharetraktor.live	0.000236	4953	4953
digimerge.net	14	syen.digimerge.net bakh.digimerge.net barx.digimerge.net aess.digimerge.net	0.015215	448	448
uromatalieslave.space	1	uromatalieslave.space	0.025195	352	352
donweb-homeip.net	13	sampleresumeformat.donweb-homeip.net zingi.donweb-homeip.net telei.donweb-homeip.net frue.donweb-homeip.net	0.000349	348	342
vpwww.bid	35	uk6.vpwww.bid 295.vpwww.bid www.1xx.vpwww.bid nln.vpwww.bid	0.237127	298	298
synterrarealty.com	1	synterrarealty.com	0.395452	296	296
ghostofsweden.se	1	www.ghostofsweden.se	0.000039	232	232
entrepots-anr.fr	18	volet-roulant-en-panne-orgerus.entrepots-anr.fr volet-roulant-en-panne-ozoir-la-ferriere.entrepots-anr.fr volet-roulant-en-panne-verrieres-le-buisson.entrepots-anr.fr volet-roulant-en-panne-meudon.entrepots-anr.fr	0.000506	216	216
pandeysfresh.in	1	www.pandeysfresh.in	0.000123	168	168
picc.info	4	ebusinessemarketing.picc.info beauty.picc.info careers.picc.info education.picc.info	0.000014	145	72

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	1202/1232	www.minpeche.gov.mg lastminutegalapagosdeals.com.greencloud.zone livezindi1.top	0.080216	14318	7159	7159
0.20	1/1	www.patagoniaimagenes.com.ar parceiros.vulcanequipamentos.com.br	0.124150	8	6	2

Dynamic DNS providers:

dn			top10m	nosfx	app	ok	nx	nx/app
	Four examples	unique	mean	mean	sum	sum	sum	mean
blg.lt	qawaq491.23.e.uni.blg.lt farap55.9.b.uni.blg.lt best305.h.ina.blg.lt guide952.2.a.uni.blg.lt	27	4552931.0	0.037108	320	164	156	0.433333
donweb-homeip.net	sampleresumeformat.donweb-homeip.net zingi.donweb-homeip.net telei.donweb-homeip.net frue.donweb-homeip.net	13	NaN	0.000349	348	342	6	0.034615
netdna-ssl.com	fixyourbrowser-brcxaoawlauo.netdna-ssl.com wigi725ylkk16hjts2tbfo9i-wpengine.netdna-ssl.com bears-rwuoyvuy.netdna-ssl.com 4egpo74mm9c32qi8c2b0tcx3-wpengine.netdna-ssl.com	13	70455.0	0.501106	212	206	6	0.034615
smart-hosting.info	olocesaze.smart-hosting.info wumukyyip.smart-hosting.info olebepi.smart-hosting.info ofeyeqyy.smart-hosting.info	12	NaN	0.000020	144	72	72	0.450000
comwp-login.php	eastwindbrokers.comwp-login.php rebranding-africa.comwp-login.php www.ankaradakarot.comwp-login.php algorytmika.comwp-login.php	10	NaN	0.000000	62	31	31	0.450000
comxmlrpc.php	nighthawksdiner.comxmlrpc.php algorytmika.comxmlrpc.php rebranding-africa.comxmlrpc.php www.ramsl-attersee.comxmlrpc.php	5	NaN	0.000000	20	10	10	0.450000

Chapter 17

[6] 8219s.exe – PWS:Win32/Zbot!GO

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	examples	nosfx mean	app sum	ok sum	nx sum
messagingengine.com	1	in1.smtp.messagingengine.com	0.000005	132827	132809	0
digitalwaves.co.nz	1	mail7.digitalwaves.co.nz	0.000006	132707	132667	0
rapstar.com	1	rapstar.com	0.000016	4033	4033	0
juno.net	1	juno.net	0.000148	4026	4026	0
honey-do-this.com	1	honey-do-this.com	0.000089	3981	1999	1982
goldcockerelbooks.co.uk	1	goldcockerelbooks.co.uk	0.000007	3948	3942	0
chataddict.com	1	chataddict.com	0.000442	3869	3863	0
kalteng.net	1	kalteng.net	0.000059	3777	3776	0
psmtp.com	440	spencertech.com.s7b1.psmtp.com spencertech.com.s7a2.psmtp.com spencertech.com.s7b2.psmtp.com spencertech.com.s7a1.psmtp.com	0.000049	2432	1688	98
avinalarf.co.uk	1	avinalarf.co.uk	0.001387	2160	2160	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	1039/1055	honey-do-this.com gcse.comgcse.com elijahsfm.com dynranver.com	9.388192e-01	29253	14653	14600
0.40	4/14	avictorias.com.bak-mx.na0108.smtbak.com ujkf uko skb	7.149568e-02	229	128	98
0.00	4/12	ALT2.ASPMX.L.GOOGLE.com ALT1.ASPMX.L.GOOGLE.com ASPMX.L.GOOGLE.com ASPMX2.GOOGLEMAIL.com	3.981831e-05	3235	2185	35
0.35	2/3	dem cpm cheapcaribbean.com.s9a2.psmtp.com	6.862965e-07	72	45	27
0.20	9/13	ylhqlrgqxgordeytindafukreqjvtw.info shuofrpvcyukzgqnjbykrvkddu.com prdqjfhwookftucvkwclhyzlyt.biz gubmpfypeisctovkgaqghircxsfqlqc.biz	4.616070e-01	108	83	25
0.30	2/6	ASPMX3.L.GOOGLE.COM ASPMX2.L.GOOGLE.COM thecmafoundation.org.s8a3.psmtp.com mbbblaw.com.s8a2.psmtp.com	2.463146e-05	54	31	18
0.25	3/3	server14.idealhost.ws m03.internetmailserver.net eaeobxgtsvsjzljwkskvcaegqyay.net	3.333945e-01	30	21	9

Dynamic DNS providers:

dn			top10m	nosfx	app	ok	nx	nx/app
	Four examples	unique	mean	mean	sum	sum	sum	mean
psmtp.com	spencertech.com.s7b1.psmtp.com spencertech.com.s7a2.psmtp.com spencertech.com.s7b2.psmtp.com spencertech.com.s7a1.psmtp.com	440	NaN	0.000049	2432	1688	98	0.025909
ukw	dem jjro comq hlp	92	NaN	0.000000	622	516	106	0.044565
arsmtp.com	abrepro.com.1.arsmtp.com becksclassic.com.2.0001.arsmtp.com abrepro.com.2.arsmtp.com becksclassic.com.1.0001.arsmtp.com	82	NaN	0.000062	510	392	8	0.015854
mxlogic.net	now-zen.com.inbound20.mxlogic.net now-zen.com.inbound10.mxlogic.net now-zen.com.inbound30.mxlogic.net redrocketnetworks.com.inbound10.mxlogic.net	40	7783504.0	0.000105	243	179	6	0.026250
outlook.com	ms99216328.msv1.invalid.outlook.com technogestass-com.mail.eo.outlook.com eliodeo-net.mail.protection.outlook.com dipolar-com-au.mail.eo.outlook.com	31	4672.0	0.000377	302	251	11	0.024194
smtproutes.com	nhbody.com.pri-mx.smtproutes.com nhbody.com.bak-mx.smtproutes.com curemark.com.pri-mx.na0103.smtproutes.com avictorias.com.pri-mx.na0108.smtproutes.com	21	NaN	0.000065	127	98	4	0.030952
serverdata.net	west.smtp.exch027.serverdata.net east.smtp.exch027.serverdata.net west.smtp.exch021.serverdata.net east.smtp.exch021.serverdata.net	18	216019.0	0.000056	182	128	8	0.011111
appriver.com	server505.appriver.com server504.appriver.com server110.appriver.com server111.appriver.com	16	439710.0	0.000055	114	88	10	0.062500
google.com	alt1.aspmx.l.google.com alt2.aspmx.l.google.com aspmx.l.google.com www.google.com	12	3.0	0.000031	268784	267931	123	0.004167
GOOGLE.COM	ASPMX3.L.GOOGLE.COM ASPMX2.L.GOOGLE.COM ALT1.ASPMX.L.GOOGLE.COM ALT2.ASPMX.L.GOOGLE.COM	6	NaN	0.000030	455	322	16	0.100000
GOOGLE.com	ALT2.ASPMX.L.GOOGLE.com ALT1.ASPMX.L.GOOGLE.com ASPMX.L.GOOGLE.com ALT3.ASPMX.L.GOOGLE.com	5	NaN	0.000031	1464	970	15	0.000000

Chapter 18

[7] nltool.exe – Backdoor:Win32/Caphaw.AH

Top 10 used DNs outside to Top10Milion list:

	dn		nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
bdn						
smis.cc	2373	smis.cc tvlvnj61g1t2j.smis.cc qr07rtf.smis.cc soy83d.smis.cc	0.032145	11660	6889	4771
pcg.su	1741	pcg.su m4xhy95w9eci4z8.pcg.su m859dl7o.pcg.su rxt3afwye90rkuw.pcg.su	0.139370	8304	4649	3651
ccl.su	1347	ccl.su 224puvd2bkwm9uq.ccl.su jv50ivmsn2w.ccl.su umrzi90t.ccl.su	0.034333	8104	5142	2824
jcy.su	58	jcy.su o6yyv8wqpehka8.jcy.su paw3lr4jv.jcy.su pxbv2w0wlhxa.jcy.su	0.476210	6769	6619	108
leq.su	59	leq.su qq3ygpu.leq.su 0sb73nc8n4jrp46.leq.su 0fevex2hpl.leq.su	0.129163	5790	5592	108
gah.cc	1	gah.cc	0.029550	4035	4035	0
kirr.cc	6	uhqdee5pj.kirr.cc w8oxg7xsxdiq82j.kirr.cc zsi1cvw00z6ass.kirr.cc 50o0y0n68afzdx42.kirr.cc	0.425517	3246	3246	0
amia.cc	24	s51gxdioelyz.amia.cc nynqugqon6.amia.cc thz146zn.amia.cc k1w92.amia.cc	0.256066	3068	3068	0
elg.cc	1	elg.cc	0.023775	2904	2904	0
ehk.su	42	4dbv4h6x36.ehk.su weno3hjp410xn2z.ehk.su 5eimvd.ehk.su 8mf1y27c7ynnd3e1d.ehk.su	0.649130	2889	2882	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	7/5520	m4xhy95w9eci4z8.pcg.su 224puvd2bkwm9uq.ccl.su tvlvnj61g1t2j.smis.cc m859dl7o.pcg.su	0.072279	11518	5759	5759
0.35	2/2	smis.cc pcg.su	0.000409	11367	7157	4210
0.25	1/1	ccl.su	0.002866	5275	3726	1411
0.00	4/4	leq.su jcy.su paly.cc sags.cc	0.001097	15745	15433	177
0.30	4/17	eztir0b4jtki.smis.cc i32yrxporlux44c.smis.cc pxbv2w0wlhxa.jcy.su igwjrsl.smis.cc	0.240463	51	34	17
0.20	2/10	1hr5cqn.smis.cc 860ds58evj804cxir.smis.cc kvtg3fqs.smis.cc x7hcmavd6q7ie5i.smis.cc	0.000479	40	26	10
0.40	1/1	0gfgg6vbj2v.smis.cc	0.000039	5	3	2

Dynamic DNS providers:

dn			top10m	nosfx	app	ok	nx	nx/app
	Four examples	unique	mean	mean	sum	sum	sum	mean
smis.cc	smis.cc tvlvnj61g1t2j.smis.cc qr07rtf.smis.cc soy83d.smis.cc	2373	NaN	0.032145	11660	6889	4771	0.435651
pcg.su	pcg.su m4xhy95w9eci4z8.pcg.su m859dl7o.pcg.su rxt3afwye90rkuw.pcg.su	1741	NaN	0.139370	8304	4649	3651	0.448679
ccl.su	ccl.su 224puvd2bkwm9uq.ccl.su jv50ivmsn2w.ccl.su umrzi90t.ccl.su	1347	NaN	0.034333	8104	5142	2824	0.449406
leq.su	leq.su qq3ygpu.leq.su 0sb73nc8n4jrp46.leq.su 0fevex2hpl.leq.su	59	NaN	0.129163	5790	5592	108	0.381356
jcy.su	jcy.su o6yyv8wqpehka8.jcy.su paw3lr4jv.jcy.su pxbv2w0wlhxa.jcy.su	58	NaN	0.476210	6769	6619	108	0.375000
paly.cc	paly.cc qch5vkyd.paly.cc 49h0rib.paly.cc iyp6np36x2e7n.paly.cc	58	NaN	0.104857	1342	1225	114	0.442241
sags.cc	sags.cc 6zmfv07tcqmpcuxy.sags.cc vj08qly0kps4.sags.cc kt1itphr5.sags.cc	6	NaN	0.330233	2206	2196	10	0.375000

Chapter 19

[19] Ferer.exe – Trojan:Win32/Emotet.G

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	examples	nosfx mean	app sum	ok sum	nx sum
upcbusiness.at	1	mail.upcbusiness.at	0.000029	604	604	0
telenet-ops.be	9	popimapnocm04-vip.telenet-ops.be popimapnocm03-vip.telenet-ops.be popimapnocm02-vip.telenet-ops.be popimaphobo04-vip.telenet-ops.be	0.000011	302	302	0
ns0.ovh.net	1	ns0.ovh.net	0.000005	274	274	0
udag.de	3	pop3.udag.de smtp.udag.de pop.udag.de	0.000013	256	256	0
patioart.ge	1	www.patioart.ge	0.000141	228	228	0
abcpartner.de	3	smtp.abcpartner.de mxsgg01.abcpartner.de mxsgg02.abcpartner.de	0.000005	178	178	0
de-nserver.de	32	server670-han.de-nserver.de server1178-han.de-nserver.de server189-han.de-nserver.de server1246-han.de-nserver.de	0.000066	154	151	3
as9143.net	1	pop-new.tb.mail.iss.as9143.net	0.000006	152	152	0
ogicom.net	28	s50-mail.ogicom.net s48-mail.ogicom.net mail26.ogicom.net s30-mail.ogicom.net	0.004083	148	148	0
alfahosting-server.de	27	alfa3019.alfahosting-server.de alfa3033.alfahosting-server.de alfa3016.alfahosting-server.de alfa3057.alfahosting-server.de	0.000114	142	142	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

	bdn/dn	dn	nosfx	app	ok	nx
	num	examples	mean	sum	sum	sum
nx/app						
0.45	128/142	resmail-prd-dc1-pop3-vip.bc pop01-cluster.nexlink.ch rs-0-237.acens.net s15.mynet.at	0.003584	496	248	248

Dynamic DNS providers:

dn			top10m	nosfx	app	ok	nx	nx/app
	Four examples	unique	mean	mean	sum	sum	sum	mean
de-nserver.de	server670-han.de-nserver.de server1178-han.de-nserver.de server189-han.de-nserver.de server1246-han.de-nserver.de	32	NaN	6.633396e-05	154	151	3	0.028125
unifiedlayer.com	192-185-109-20.unifiedlayer.com 192-185-56-171.unifiedlayer.com 192-185-140-17.unifiedlayer.com 192-185-73-12.unifiedlayer.com	26	1726368.0	9.949256e-07	54	36	18	0.294231
stratoserver.net	h1317164.stratoserver.net h2182887.stratoserver.net h2270882.stratoserver.net h2163760.stratoserver.net	17	3173527.0	4.781001e-06	58	57	1	0.026471
aruba.it	mxavas.aruba.it mxd3.aruba.it host100-195-58-185.serverdedicati.aruba.it host212-249-110-95.serverdedicati.aruba.it	15	49973.0	1.012427e-05	310	298	12	0.120000
onlinehome-server.info	s15346846.onlinehome-server.info s15381387.onlinehome-server.info s15416893.onlinehome-server.info s16918063.onlinehome-server.info	15	791920.0	1.719458e-05	86	84	2	0.060000
natrohost.com	cluster11.natrohost.com cluster06.natrohost.com cluster09.natrohost.com cluster18.natrohost.com	13	9845487.0	3.731183e-06	60	36	24	0.380769
whmpanels.com	server-0094i00.whmpanels.com server-0141.whmpanels.com server-0158.whmpanels.com uamt.whmpanels.com	9	NaN	7.303830e-06	52	51	1	0.050000
superhosting.bg	host-195-191-149-35.superhosting.bg host125-139.superhosting.bg host125-137.superhosting.bg host-164-138-219-75.superhosting.bg	9	1989792.0	1.857128e-06	18	10	8	0.400000
versatel.de	mx01.versatel.de mx02.versatel.de maildo.versatel.de ens44fl.versatel.de	6	2014510.0	1.032131e-04	146	78	68	0.150000
inmotionhosting.com	ecbiz60.inmotionhosting.com vps5296.inmotionhosting.com dedicated2073.inmotionhosting.com biz104.inmotionhosting.com	5	3864.0	9.445311e-06	10	9	1	0.090000

Chapter 20

[20] Ferer.exe/9049.exe – Trojan:Win32/Emotet.G

Top 10 used DNs outside to Top10Milion list:

bdn	dn num	examples	nosfx mean	app sum	ok sum	nx sum
patioart.ge	1	www.patioart.ge	0.000141	216	216	0
atlantadultcare.com	2	atlantadultcare.com www.atlantadultcare.com	0.000137	56	56	0
gouliami.gr	1	gouliami.gr	0.000618	52	52	0
rbgstyle.com	1	eshop.rbgstyle.com	0.000002	48	48	0
jffjff.com	1	jffjff.com	0.023716	48	48	0
alsoknownas-blog.com	1	alsoknownas-blog.com	0.000018	40	40	0
drwallach90.com	1	drwallach90.com	0.000002	40	40	0
maximum.pl	1	incus.projekty.maximum.pl	0.000021	34	34	0
ericafrances.co.uk	1	www.ericafrances.co.uk	0.039345	34	34	0
upcbusiness.at	1	mail.upcbusiness.at	0.000029	30	30	0

DNs having NX responses greater than 0, grouped by their NX/app ratio:

nx/app	bdn/dn num	dn examples	nosfx mean	app sum	ok sum	nx sum
0.45	15/15	servcila2.cilamexeua.gob.mx fire.bertele.priv ip-129-121-205-66.local resmail-prd-dc1-pop3-vip.bc	0.003073	30	15	15

Dynamic DNS providers:

dn		top10m	nosfx	app	ok	nx	nx/app
Four examples	unique	mean	mean	sum	sum	sum	mean
aruba.it							
host133-131-235-85.serverdedicati.aruba.it mxavas.aruba.it smtp-pc.aruba.it mxd7.aruba.it	8	49973.0	0.000012	28	26	2	0.1125
strato.de							
stmp.strato.de imap.strato.de post.strato.de smtp.strato.de	5	23554.0	0.000004	124	123	1	0.0900