

The DGA of Simda/Shiz

 bin.re/blog/the-dga-of-simda-shiz/



Only when I had already finished the DGA of Simda/Shiz, I noticed that [DGArchive](#) and [Abuse.ch](#) analysed Simda's DGA before me. All this entry contributes are two additional seeds.

The length, top level domain, and the key vary from sample to sample. For the domain generation, only the sum of the key's character matter, the key itself is irrelevant.

set	base	domain length	tld	key	key sum	first 10 domains
1	45AE94B2	7	com	1676d5775e05c50b46baa5579d4fc7	2052	gatyfus.com, lyvyxor.com, vojyqem.com, qetyfuv.com, puvyxil.com, gahyqah.com, lyryfyd.com, vocyzit.com, qegyqaq.com, purydyv.com
2	45AE94B2	5	eu	1670cf21500911e1758e2b0dd5b4	1824	lykef.eu, qekol.eu, galin.eu, volup.eu, puzej.eu, lyxav.eu, qexor.eu, gacuf.eu, vocyz.eu, puvem.eu
3	45AE94B2	7	info	167cd47c0a09c9036d6097b754ab2e73	2146	qebevil.info, citocec.info, jejudin.info, divywew.info, wetavop.info, vojokyf.info, lyvudoj.info, fotryz.info, ryhabov.info, novolym.info

set	base	domain length	tld	key	key sum	first 10 domains
4	45AE94B2	7	info	?	2038	puwedyp.info, tulokuq.info, rypubuv.info, rycyril.info, wedafog.info, qebolap.info, qeguneq.info, mamytec.info, najagyk.info, noroxuf.info
5	45AE94B2	11	eu	1670cf215403c56d8859a0636ffc74	1952	cihunemyror.eu, digivehusyd.eu, vofozymufok.eu, fodakyhijyv.eu, nopegymozow.eu, gatedyhavyd.eu, marytymenok.eu, jewuqyjywyv.eu, qqinuqypoq.eu, kemocujufys.eu
5	45AE94B2	11	eu	1670cf215403c56d8859a0636ffc74	1952	cihunemyror.eu, digivehusyd.eu, vofozymufok.eu, fodakyhijyv.eu, nopegymozow.eu, gatedyhavyd.eu, marytymenok.eu, jewuqyjywyv.eu, qqinuqypoq.eu, kemocujufys.eu
6	45AE94B2	7	info	?	2182	lyromex.info, maxenem.info, dosuves.info, xubaxej.info, wehyzav.info, gaqokaw.info, vilehaf.info, tupigal.info, jevadan.info, nofupat.info

I have not had access to a sample for the fourth and sixth seed, but found the key sum to be 2038 by brute forcing. [Here](#) is a Python script of the DGA that contains these five seeds.