The DGA of Simda/Shiz

Archived: 2026-04-05 17:30:13 UTC

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 DGA

The DGA is pretty simple:

```
 length = 7
tld = "com"
key = "1676d5775e05c50b46baa5579d4fc7"
base = 0x45AE94B2

consonants = "qwrtpsdfghjklzxcvbnmv"
vowels = "eyuioa"

step = 0
for m in key:
    step += ord(m)

for nr in range(1000):
    domain = ""
    base += step

    for i in range(length):
        index = int(base/(3+2*i))
        if i % 2 == 0:
            char = consonants[index % 20]
        else:
            char = vowels[index % 6]
        domain += char

    domain += "." + tld
    print(domain)
```

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.

The Seeds

I found five different sets of seeds + one on virustracker:

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, citokec.info, jejudin.info, divywew.info, wetavop.info, vojokyf.info, lyvudoj.info, fotyryz.info, ryhabov.info, novolym.info
4	45AE94B2	7	info	?	2038	puwedyp.info, tulokuq.info, rypubuv.info, rycyril.info, wedafog.info, qebolap.info, qeguneq.info, mamytec.info,

set	base	domain length	tld	key	key sum	first 10 domains
						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, qeqinuqypoq.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, qeqinuqypoq.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.

Samples on Malwr.com

The following table lists samples from malwr.com that use the DGA of Simda/Shiz:

md5	analysis date	set	Kaspersky	Microsoft	Symantec
9c5e9e1a049ec198abf461f92758d8b5	14 May. 2013	1	Shiz.raj	Injector.gen!BQ	(c)
ecbdcf103052f1537798e5b27e1f2538	26 Aug. 2013	3	Shiz.afai	Simda.gen!B	WS.Reputation.1
d0acd37e9075990d0f1289db350c258d	08 Nov. 2013	1	(c)	Simda.AF	Shiz!gen
c4d1a029de33208a56eba8f5fe8b6eb2	03 Feb. 2014	5	(g)	(c)	(c)
1fde0e0a2b16fcb4c483ec7ed8531756	19 Mar. 2014	5	(g)	Injector.TH	Shiz!gen
1fde0e0a2b16fcb4c483ec7ed8531756	19 Mar. 2014^{R}	5	(g)	Injector.TH	Shiz!gen
fdcab35a4d38deb9d41a3c1f12075d22	23 Mar. 2014	5	Shiz.aklr	Injector.TH	(c)
7070ac6706e345e75103054a4f30ff4d	26 Mar. 2014	5	?	?	?
71ca5168b13f6657f79c9d43ed448372	30 Mar. 2014	3	(g)	Simda.gen!F	
0972ebba0a8f21f930c7e2f27be96646	29 May. 2014	1	(g)	Simda.D	WS.Reputation.1
39f2998a165cb2f5986bf288e7153490	30 May. 2014	1	Shiz.tiq	Simda	WS.Reputation.1
03b7288ba9876ad4e80074ab95cb889f	22 Jun. 2014	5	(g)	Simda	Shiz!gen2
301eb56db2e5e601453da34698f9db1b	25 Jun. 2014	5	(g)	Simda	WS.Reputation.1
0537c9f2dc45b10be4c276600f7af035	26 Jun. 2014	1	Shiz.raj	Simda.G	Malcol

md5	analysis date	set	Kaspersky	Microsoft	Symantec
02f6cb7a90169b8569133a75a74e9ba0	27 Jun. 2014	5	(g)	(c)	(g)
10708d7d77ab864f1d38fe1b6161422d	29 Jun. 2014	5	(g)	Simda	(g).2
11b54c5d8531c0705d30a87f2b42a20f	29 Jun. 2014	4	Shiz.cxgu	Simda	WS.Reputation.1
12a92f800239af5e715842d6fcf7c82c	30 Jun. 2014	5	(g)	Obfuscator.WY	(g).2
14ce26edf8ccf4b5dc6e8170ecc04a82	01 Jul. 2014	5	(g)	Simda.AA	(c)
174b8b6048cc18e069a633786ead5cc3	01 Jul. 2014	5	(g)	Simda	FakeAV
196e7f6c572a2ea7afcc322530f8f970	01 Jul. 2014	3	(g)	Simda.gen!F	WS.Reputation.1
25c9bb91088b6062ac5ce8d214cd93a5	03 Jul. 2014	5	(g)	Obfuscator.ZV	Shiz!gen2
34920722bdfe2ce5cff7e2f692939666	05 Jul. 2014	1	Shiz.raj	Simda	WS.Reputation.1
564dff857b3c0c3ef304df86d69dbe4d	13 Jul. 2014	5	(g)	Simda.X	(g)
575401b07ccec2f84ff6e46d26a84dc5	14 Jul. 2014	5	(g)	(c)	(c)
7b9d6e2d8a0a0b20d493ea2f37de260d	18 Jul. 2014	1	(g)	Simda.P	Shiz!gen
7974fb86000385219d4b9cd63bcb0d2f	20 Jul. 2014	5	(g)	Obfuscator.ZV	Shiz!gen2
7df9185319e4877fc0322bdf56af89bc	20 Jul. 2014	5	?	Simda	Shiz!gen2
809652095b88a2fa0ea4dd89760599c1	21 Jul. 2014	2	(g)	Simda.AF	Shiz!gen

md5	analysis date	set	Kaspersky	Microsoft	Symantec
83f2ad344ca7225cb675c03d0c66a0b6	21 Jul. 2014	5	(g)	Simda	WS.Reputation.1
8b7000002d47146d7d7e7ba2c5b3d120	22 Jul. 2014	5	(g)	Simda	Shiz
9977d2b1b279112cc1024858802b3ab8	23 Jul. 2014	5	(g)	Simda.U	(g)
ad71cd5a05db9473c5580eb070963bf9	02 Mar. 2015	1	(g)	Simda.AF	Shiz!gen

(g): generic, ?: not scanned, (c): clean
