Dridex v4 - Configuration Files, Network and Binaries

viql.github.io/dridex/

What is this Website?

This website lists configuration files, supernodes and modules of the **Dridex v4** malware. The collection includes data from these 7 botnets:

- 23005
- 11122
- 10105
- 7200
- 4200
- 3122
- 2144

Some of the information is also available as Suricata rules, Yara rules and CSV lists, see Exports . The displayed information does have the aspiration to completeness, actuality, or quality. Use the information at your own discretion. All timestamps are given in UTC.

Configs

Dridex is configured with configuration files. These files specify, among other things, which website urls should be redirected and where. The targets of the redirects are also listed in section redirects. Now and then, the config files also deliver new *supernodes*. Those are separately listed in the supernodes section.

The configuration files can also deliver executables. Those are listed in section modules. The *modules* blocks originally contained full binaries. I replaced them with hashes. All modules in Dridex are identified by crc32 checksums, when known, the "name" matching the CRC32 is also listed. Neither the hashes, nor name are part of the config delivered by Dridex.

In version 3 of Dridex, the configuration files where delivered in XML format with descriptive tag and attribute names. In the current version 4, the configuration is delivered in a binary format without the helpful textual hints as to what the fields do. I tried to replicate the format from v3 as good as possible, but not all fields might be named appropriately.

Only config files from the last 90 days are shown.

timestamp	botnet	view
2018-06-25 09:42:10	11122	show

timestamp	botnet	view
2018-06-23 07:55:04	10105	show
2018-06-22 23:40:07	10105	show
2018-06-12 10:52:10	11122	show
2018-06-08 07:35:06	10105	show
2018-05-28 10:00:04	2144	show
2018-05-28 10:00:04	11122	show
2018-05-24 12:40:05	11122	show
2018-05-24 12:40:05	2144	show
2018-05-23 13:20:04	11122	show
2018-05-23 13:20:04	2144	show
2018-05-22 09:00:06	2144	show
2018-05-19 20:20:06	11122	show
2018-05-09 06:40:03	2144	show
2018-05-09 06:40:03	11122	show
2018-05-09 06:30:04	11122	show
2018-05-07 10:30:06	2144	show
2018-05-07 10:30:06	11122	show
2018-05-01 21:10:05	11122	show
2018-05-01 21:10:04	2144	show
2018-04-03 14:40:11	11122	show

Network

Redirect Servers

Traffic to the targeted websites is redirected to servers controlled by the Dridex operators. The following table shows servers from the config files of the last 180 days.

ip	port	botnet	added	last seen in config
67.212.161.142	443	10105	2018-06-23 07:55:04	current config
178.62.36.31	443	10105	2018-06-22 23:40:07	2018-06-22 23:40:07
104.236.189.165	443	10105	2018-06-08 07:35:06	current config
178.62.103.94	443	10105	2018-06-08 07:35:06	2018-06-08 07:35:06
74.221.221.59	1234	2144, 11122	2018-05-28 10:00:04	current config
162.248.221.126	8443	2144, 11122	2018-05-23 13:20:04	2018-05-24 12:40:05
52.19.152.75	443	2144	2018-05-22 09:00:06	2018-05-22 09:00:06
45.76.121.12	3889	2144, 11122	2018-05-09 06:30:04	current config
78.47.47.196	443	7200	2018-04-09 18:20:36	2018-04-09 18:20:36
92.207.100.244	4843	7200	2018-04-03 21:40:22	current config
104.131.187.88	4143	2144, 3122, 11122	2018-04-03 14:40:11	2018-04-03 14:40:11
46.105.131.70	443	2144, 3122, 4200, 7200, 11122	2018-04-03 13:10:22	2018-04-03 14:40:11
121.84.151.68	443	4200	2018-04-03 08:00:22	2018-04-03 08:00:22
46.105.131.76	443	4200, 7200	2018-04-03 08:00:22	current config
178.63.84.81	443	2144, 3122, 4200, 11122	2018-04-03 08:00:13	2018-05-19 20:20:06
45.55.25.107	3889	2144, 3122, 11122	2018-04-03 08:00:13	2018-05-23 13:20:04

ip	port	botnet	added	last seen in config
133.242.208.183	443	23005	2018-04-02 09:10:19	current config
220.227.247.39	443	23005	2018-03-26 17:20:24	2018-04-03 02:02:24
104.131.44.150	443	23005	2018-03-12 12:50:19	2018-03-13 10:19:22
62.75.148.105	443	2144, 3122	2018-03-10 04:50:10	2018-03-14 19:50:12
51.255.49.240	3889	4200, 7200	2018-03-06 02:00:18	2018-04-09 18:20:36
45.32.87.122	443	4200	2018-03-05 19:10:32	2018-03-05 19:30:16
67.207.142.38	4431	4200, 7200	2018-02-22 01:00:22	current config
178.62.140.5	443	23005	2018-02-22 00:40:27	2018-03-28 12:50:17
178.62.12.13	443	23005	2018-02-21 18:10:46	current config
198.199.98.88	443	2144, 3122, 4200	2018-02-21 15:00:15	2018-03-21 18:10:29
45.55.201.174	8443	4200	2018-02-17 16:50:15	2018-03-21 18:20:21
37.228.151.216	443	4200	2018-02-17 16:50:15	2018-02-28 20:30:19
178.62.232.185	443	2144, 3122	2018-02-17 15:50:11	2018-03-29 11:15:12
216.51.232.176	4043	2144, 4200	2018-02-17 15:50:11	current config
178.33.109.227	443	2144, 3122, 4200	2018-02-17 15:50:11	2018-03-29 11:15:12
88.198.99.27	4143	23005	2018-02-17 12:00:25	2018-03-10 19:20:22

ip	port	botnet	added	last seen in config
139.59.185.21	443	23005	2018-02-17 12:00:25	2018-04-02 01:20:18

Supernodes

Supernodes are ordinary infected clients, that were "promoted" by Dridex to relay traffic of regular infected clients. The owners of the IPs are in no way related to the Dridex operation. Do not block these IP addresses, only use them to detect Dridex infections in your own network.

The supernodes from the last 100 days. The columns *added* and *removed* show the time whenthe supernodes appeared in and disappeared from a config file. The columns *firstseen* and *lastseen* show when the supernode last responded to a Dridex ping. These pings are encrypted by the Dridex network protocol, hence, responding clients arealmost certainly infected by Dridex.Those marked with "" were active with the last 3 days, i.e.,either responded to a ping or were seen in Dridex config. those with "" were inactive.

st.	ip	port	botnet	added	removed	firstseen	lastseen
	91.84.15.17	443	2144, 11122	2018-06-11 14:05:44		2018-05-29 08:47:46	2018-07-19 13:57:44
	5.226.111.135	444	4200, 7200	2018-04-05 11:51:39		2018-04-01 19:45:40	2018-07-19 13:55:24
	207.47.95.202	443	2144, 11122	2018-06-11 14:05:44		2018-06-07 15:49:51	2018-07-19 13:51:52
	81.130.208.120	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 09:49:13	2018-07-19 13:50:09
	80.2.118.90	443	2144, 11122	2018-06-11 14:05:44		2018-06-04 13:43:52	2018-07-19 13:49:08
	67.84.204.83	443	2144, 3122, 11122	2018-02-05 15:11:11		2018-02-05 15:11:11	2018-07-19 13:47:41

st.	ip	port	botnet	added	removed	firstseen	lastseen
	193.251.189.134	443	2144, 3122, 11122	2018-04-07 03:10:24	2018-06-07 14:39:10	2018-02-05 15:09:35	2018-07-19 13:45:10
	216.14.144.190	443	2144, 11122	2018-06-11 14:05:44		2018-06-02 17:39:58	2018-07-19 04:07:49
	24.234.234.212	443	2144, 11122	2018-06-11 14:05:44		2018-06-04 11:35:29	2018-07-19 00:00:59
	81.133.199.158	443	2144, 11122	2018-06-11 14:05:44		2018-05-29 13:47:24	2018-07-18 15:12:08
	82.9.114.19	443	2144, 11122	2018-06-11 14:05:44		2018-05-29 08:44:54	2018-07-17 11:15:55
	69.14.75.158	443	2144, 11122	2018-06-11 14:05:44		2018-05-27 08:46:49	2018-07-13 20:22:57
	104.37.213.132	443	10105	2018-06-07 11:38:16		2018-06-07 11:38:16	2018-07-13 01:39:26
	80.235.149.254	443	2144, 11122	2018-06-11 14:05:44		2018-06-07 15:50:04	2018-07-12 15:17:22
	87.114.93.29	8443	2144, 11122	2018-06-11 14:05:44		2018-05-28 14:41:27	2018-07-12 03:09:48
	184.183.29.147	443	2144, 4200, 7200, 11122	2018-03-14 03:15:20	2018-06-07 14:39:10	2018-02-15 20:45:26	2018-07-12 00:05:34
	195.123.214.147	443	2144, 11122	2018-06-11 14:05:44		2018-05-04 23:40:35	2018-07-10 16:57:58
	185.236.77.228	443	2144, 11122	2018-06-11 14:05:44		2018-05-04 23:38:51	2018-07-10 16:54:52

st.	ip	port	botnet	added	removed	firstseen	lastseen
	80.80.184.65	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-12 17:40:03	2018-07-06 22:40:23
	92.27.84.44	443	2144, 11122	2018-06-11 14:05:44		2018-05-30 13:37:01	2018-07-06 10:53:35
	132.204.222.210	443	2144, 11122	2018-06-11 14:05:44		2018-05-28 16:42:57	2018-07-01 13:45:01
	89.168.230.187	443	2144, 11122	2018-06-11 14:05:44		2018-06-26 07:40:20	2018-06-30 19:40:40
	174.111.41.39	8443	2144, 11122	2018-06-11 07:05:15	2018-06-11 09:05:41	2018-06-15 07:50:55	2018-06-27 16:50:45
	90.208.80.182	443	2144, 11122	2018-06-11 14:05:44	2018-06-07 14:39:10	2018-06-03 22:40:22	2018-06-26 16:42:47
	77.102.48.202	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:38:07	2018-06-26 16:39:43
	188.213.31.152	443	10105	2018-06-25 19:07:11		2018-06-20 22:37:48	2018-06-26 04:38:04
	82.45.232.190	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 17:53:40	2018-06-25 13:55:33
	82.27.58.162	443	2144, 11122	2018-06-11 14:05:44		2018-05-28 14:39:45	2018-06-25 10:53:49
	70.34.1.232	443	2144, 11122	2018-06-11 14:05:44		2018-06-07 15:46:05	2018-06-25 10:46:20
	188.213.31.152	783	10105	2018-06-25 19:07:11		2018-06-20 22:37:38	2018-06-23 19:37:53

st.	ip	port	botnet	added	removed	firstseen	lastseen
	154.0.173.249	448	10105	2018-06-25 19:07:11	2018-06-20 22:07:09	2018-06-23 01:37:15	2018-06-23 01:37:15
	89.242.6.199	443	2144, 11122	2018-06-11 14:05:44		2018-05-29 12:37:18	2018-06-22 07:41:38
	154.0.173.249	783	10105	2018-06-25 19:07:11		2018-06-12 22:38:52	2018-06-21 04:40:13
	51.52.205.221	443	2144, 11122	2018-06-11 14:05:44		2018-05-27 08:36:03	2018-06-19 16:40:30
	72.209.197.73	443	10105	2018-06-18 10:07:13	2018-06-20 22:07:09	2018-06-18 04:38:07	2018-06-18 22:38:07
	67.221.213.4	443	10105	2018-06-17 01:07:20	2018-06-17 22:07:14	2018-06-17 13:37:43	2018-06-18 19:37:44
	74.139.90.161	443	10105	2018-06-18 10:07:13	2018-06-20 22:07:09	2018-06-18 10:07:13	2018-06-18 10:07:13
	71.190.144.211	443	10105	2018-06-18 10:07:13	2018-06-20 22:07:09	2018-06-18 10:07:13	2018-06-18 10:07:13
	184.189.75.254	443	10105	2018-06-18 10:07:13	2018-06-20 22:07:09	2018-06-18 01:37:25	2018-06-18 01:37:25
	76.102.216.95	443	10105	2018-06-18 10:07:13	2018-06-20 22:07:09	2018-06-12 22:38:30	2018-06-17 19:38:37
	160.124.67.77	443	10105	2018-06-18 10:07:13	2018-06-20 22:07:09	2018-06-07 11:38:04	2018-06-17 10:38:28
	160.124.67.80	448	10105	2018-06-20 22:07:09	2018-06-21 10:07:09	2018-06-07 11:37:48	2018-06-17 10:38:17

st.	ip	port	botnet	added	removed	firstseen	lastseen
	24.2.244.215	443	10105	2018-06-17 22:07:14	2018-06-18 10:07:13	2018-06-14 22:38:18	2018-06-17 07:38:39
	73.119.188.9	443	10105	2018-06-17 01:07:20	2018-06-17 22:07:14	2018-06-17 01:07:20	2018-06-17 01:07:20
	24.112.87.93	443	10105	2018-06-17 01:07:20	2018-06-17 22:07:14	2018-06-13 07:37:23	2018-06-13 10:37:27
	73.139.14.232	443	2144, 11122	2018-06-11 07:05:15	2018-06-11 09:05:41	2018-05-29 13:42:02	2018-06-13 04:48:35
	74.143.110.82	8443	10105	2018-06-07 11:38:33		2018-06-07 11:38:33	2018-06-13 01:38:49
	24.155.35.236	443	10105	2018-06-17 01:07:20	2018-06-17 22:07:14	2018-06-12 22:37:36	2018-06-13 01:37:35
	73.233.171.254	443	10105	2018-06-13 01:07:08	2018-06-14 10:07:20	2018-06-13 01:07:08	2018-06-13 01:07:08
	143.159.19.227	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 13:39:43	2018-06-12 18:39:54
	92.8.136.99	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 09:43:37	2018-06-11 16:44:30
	92.13.241.60	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	176.35.107.166	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	81.140.19.98	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44

st.	ip	port	botnet	added	removed	firstseen	lastseen
	199.189.242.179	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	87.114.97.142	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	80.88.212.194	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	87.112.70.20	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	2.49.171.60	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	64.130.133.20	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	47.208.207.12	443	2144, 11122	2018-06-11 14:05:44		2018-06-11 14:05:44	2018-06-11 14:05:44
	24.88.237.198	443	2144, 11122	2018-06-11 14:05:44	2018-06-07 14:39:10	2018-05-29 13:43:53	2018-06-11 12:55:29
	160.124.67.80	443	10105	2018-06-07 11:38:22		2018-06-09 22:37:48	2018-06-11 07:37:56
	76.113.237.214	443	2144, 11122	2018-06-11 07:05:15	2018-06-11 09:05:41	2018-06-11 07:05:15	2018-06-11 07:05:15
	85.95.118.248	443	2144, 11122	2018-06-11 07:05:15	2018-06-11 09:05:41	2018-06-11 07:05:15	2018-06-11 07:05:15
	216.14.150.89	443	2144, 11122	2018-06-11 07:05:15	2018-06-11 09:05:41	2018-06-11 07:05:15	2018-06-11 07:05:15

st.	ip	port	botnet	added	removed	firstseen	lastseen
	74.67.104.109	443	2144, 11122	2018-06-11 07:05:15	2018-06-11 09:05:41	2018-06-11 07:05:15	2018-06-11 07:05:15
	82.7.217.182	443	2144, 11122	2018-06-11 14:05:44	2018-06-07 14:39:10	2018-06-09 21:39:47	2018-06-09 22:39:38
	92.8.136.21	443	2144, 11122	2018-06-11 07:05:15	2018-06-11 09:05:41	2018-06-08 12:51:09	2018-06-08 14:49:29
	90.42.34.194	443	2144, 11122	2018-06-11 14:05:44		2018-06-08 12:43:35	2018-06-08 14:42:26
	176.35.83.72	443	2144, 11122	2018-06-08 11:05:12	2018-06-08 12:05:43	2018-06-08 11:05:12	2018-06-08 11:05:12
	73.90.23.131	443	2144, 11122	2018-06-08 11:05:12	2018-06-08 12:05:43	2018-06-08 11:05:12	2018-06-08 11:05:12
	69.31.155.9	443	2144, 11122	2018-06-08 11:05:12	2018-06-08 12:05:43	2018-06-08 11:05:12	2018-06-08 11:05:12
	24.189.208.191	443	2144, 11122	2018-06-08 11:05:12	2018-06-08 12:05:43	2018-06-08 11:05:12	2018-06-08 11:05:12
	5.151.60.105	443	2144, 11122	2018-06-08 11:05:12	2018-06-08 12:05:43	2018-06-08 11:05:12	2018-06-08 11:05:12
	90.42.22.58	443	2144, 11122	2018-06-08 11:05:12	2018-06-08 12:05:43	2018-06-08 05:52:34	2018-06-08 05:52:34
	92.19.124.255	443	2144, 11122	2018-06-08 11:05:12	2018-06-08 12:05:43	2018-06-07 15:37:24	2018-06-07 16:37:21
	188.28.181.62	443	2144, 11122	2018-06-11 14:05:44		2018-06-07 15:52:00	2018-06-07 15:52:00

st.	ip	port	botnet	added	removed	firstseen	lastseen
	46.208.1.95	443	2144, 11122	2018-06-11 07:05:15	2018-06-11 09:05:41	2018-05-29 13:40:54	2018-06-06 22:36:41
	70.34.13.206	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-04 16:49:55	2018-06-06 10:49:34
	92.237.177.28	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-04 10:36:54	2018-06-05 10:36:53
	98.145.188.243	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-03 20:35:53	2018-06-03 21:35:49
	81.254.37.45	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-05-23 02:35:59	2018-06-03 07:46:25
	151.228.203.95	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	67.10.59.91	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	24.228.72.116	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	23.251.18.85	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	120.150.176.33	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	109.21.222.28	443	2144, 3122, 11122	2018-04-07 03:10:24	2018-06-07 14:39:10	2018-04-07 03:10:24	2018-06-02 17:05:22
	95.208.30.243	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22

st.	ip	port	botnet	added	removed	firstseen	lastseen
	76.112.27.179	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	46.32.48.210	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	212.139.237.143	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	23.241.212.249	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	100.1.200.10	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	82.38.157.232	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	79.79.49.12	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	82.26.59.237	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	86.147.22.101	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-06-02 17:05:22	2018-06-02 17:05:22
	41.193.159.41	443	4200, 7200	2018-04-05 11:51:58		2018-03-18 21:45:41	2018-06-01 09:55:38
	70.34.11.145	443	2144, 11122	2018-05-30 13:05:44	2018-06-02 17:05:22	2018-05-29 13:35:39	2018-06-01 01:35:39
	137.99.236.149	443	2144, 11122	2018-05-30 13:05:44	2018-06-02 17:05:22	2018-05-30 13:05:44	2018-05-30 13:05:44

st.	ip	port	botnet	added	removed	firstseen	lastseen
	212.159.160.208	443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-05-27 08:37:46	2018-05-30 08:37:27
	50.206.15.189	8443	2144, 11122	2018-06-02 17:05:22	2018-06-07 14:39:10	2018-05-04 23:36:59	2018-05-25 13:36:58
	24.192.173.97	443	2144, 11122	2018-05-25 03:05:44	2018-05-27 08:05:57	2018-05-25 03:05:44	2018-05-25 03:05:44
	217.125.29.12	444	2144, 11122	2018-05-25 03:05:44	2018-05-27 08:05:57	2018-05-25 03:05:44	2018-05-25 03:05:44
	116.73.18.59	443	2144, 11122	2018-05-25 03:05:44	2018-05-27 08:05:57	2018-05-25 03:05:44	2018-05-25 03:05:44
	99.229.216.212	443	2144, 11122	2018-05-25 03:05:44	2018-05-27 08:05:57	2018-05-25 03:05:44	2018-05-25 03:05:44
	137.99.122.155	443	2144, 11122	2018-05-25 03:05:44	2018-05-27 08:05:57	2018-05-07 16:41:21	2018-05-16 14:41:35
	137.118.165.215	443	3122	2018-02-05 15:10:19		2018-05-16 13:46:56	2018-05-16 13:46:56
	50.251.187.217	443	2144, 3122, 11122	2018-04-07 03:10:24	2018-05-08 06:05:43	2018-02-05 15:08:53	2018-05-11 20:43:55
	212.32.242.204	443	2144, 11122	2018-05-25 03:05:44	2018-05-27 08:05:57	2018-05-04 23:36:36	2018-05-10 05:36:24
	174.109.201.186	443	23005	2018-02-16 06:20:07	2018-02-16 13:20:09	2018-02-05 15:40:08	2018-05-09 11:51:12
	104.231.38.241	443	4200, 7200	2018-04-05 11:53:20		2018-02-15 20:46:52	2018-05-09 04:47:25

st.	ip	port	botnet	added	removed	firstseen	lastseen
	37.153.92.6	444	2144, 3122, 11122	2018-03-29 19:10:22	2018-05-23 02:05:34	2018-03-19 13:41:12	2018-05-07 14:47:55
	37.153.92.6	1443	2144, 11122	2018-05-25 03:05:44	2018-05-27 08:05:57	2018-05-05 04:37:05	2018-05-05 04:37:05
	68.202.93.198	443	2144, 3122, 11122	2018-02-23 03:10:16	2018-02-27 16:05:30	2018-02-27 17:38:36	2018-05-04 16:39:54
	76.184.3.225	443	23005	2018-04-06 14:20:16		2018-02-05 15:40:30	2018-05-02 19:51:54
	66.186.52.2	443	23005	2018-04-06 14:20:16		2018-03-18 21:52:06	2018-04-30 16:52:00
	71.98.248.128	443	23005	2018-02-16 06:20:07	2018-02-16 13:20:09	2018-02-05 15:40:51	2018-04-27 17:51:39
	81.254.168.177	443	2144, 3122, 11122	2018-04-07 03:10:24	2018-05-23 02:05:34	2018-02-14 10:36:15	2018-04-23 16:41:36
	172.249.88.69	443	2144, 3122, 11122	2018-03-29 19:10:22	2018-06-07 14:39:10	2018-02-05 19:43:17	2018-04-12 10:46:04
	37.153.92.6	8443	2144, 3122, 11122	2018-03-29 19:10:22	2018-05-27 08:05:57	2018-03-19 08:36:47	2018-04-11 14:41:53
	75.128.238.38	443	4200, 7200	2018-03-14 03:15:20	2018-04-01 19:15:19	2018-02-15 20:46:19	2018-04-11 02:56:30
	98.127.252.183	443	2144, 3122, 11122	2018-03-15 09:10:15	2018-03-20 13:10:15	2018-02-05 15:12:06	2018-04-09 16:48:34
	212.237.42.204	443	2144, 3122, 11122	2018-04-07 03:10:24	2018-05-27 08:05:57	2018-03-18 21:26:36	2018-04-07 12:44:34

st.	ip	port	botnet	added	removed	firstseen	lastseen
	43.231.250.172	3389	23005	2018-04-06 14:20:16		2018-04-06 14:20:16	2018-04-06 14:20:16
	179.108.87.11	443	4200, 7200	2018-04-05 11:52:27		2018-04-05 20:15:17	2018-04-05 20:15:17
	41.193.159.41	444	4200, 7200	2018-04-05 11:52:26		2018-04-05 20:15:17	2018-04-05 20:15:17
	151.0.179.218	8443	4200, 7200	2018-04-05 11:53:40		2018-04-01 19:47:39	2018-04-05 08:47:49
	104.34.220.68	443	2144, 3122, 11122	2018-03-30 21:11:47	2018-04-03 12:05:50	2018-02-05 15:07:31	2018-04-03 12:41:21
	73.138.81.95	443	2144, 3122, 11122	2018-03-30 21:11:47	2018-04-03 12:05:50	2018-03-30 21:11:47	2018-04-01 12:05:56
	47.42.53.110	443	4200, 7200	2018-04-05 11:52:48		2018-02-15 20:46:30	2018-03-29 13:46:33
	71.41.24.246	443	2144, 3122, 11122	2018-03-23 18:05:37	2018-03-23 21:10:14	2018-03-23 18:05:37	2018-03-23 18:10:10
	24.239.82.73	443	23005	2018-02-16 06:20:07	2018-02-16 13:20:09	2018-02-17 16:51:51	2018-03-23 17:51:27
	66.65.47.220	443	2144, 3122, 11122	2018-04-01 12:05:56	2018-04-04 02:10:17	2018-02-05 15:10:07	2018-03-23 17:45:36
	184.186.193.162	443	2144, 3122, 11122	2018-02-05 15:09:25		2018-02-14 09:37:08	2018-03-23 17:44:31
	217.13.106.51	443	23005	2018-03-28 15:20:21	2018-03-31 18:20:18	2018-02-05 15:39:34	2018-03-23 15:50:36

st.	ip	port	botnet	added	removed	firstseen	lastseen
	91.110.73.48	443	4200, 7200	2018-03-14 03:15:20	2018-04-01 19:15:19	2018-03-19 08:47:25	2018-03-22 14:47:21
	108.205.215.92	443	2144, 3122, 11122	2018-03-15 09:10:15	2018-03-20 13:10:15	2018-02-05 15:09:04	2018-03-20 09:44:05
	51.52.81.84	443	4200	2018-02-05 15:28:57		2018-02-05 15:28:57	2018-03-19 08:45:26
	74.66.65.127	443	2144, 3122, 11122	2018-03-15 09:10:15	2018-03-20 13:10:15	2018-02-05 22:44:44	2018-03-18 16:05:24
	91.189.43.152	443	2144, 3122, 11122	2018-03-15 09:10:15	2018-03-20 13:10:15	2018-03-15 09:10:15	2018-03-18 16:05:24
	139.78.21.232	443	2144, 3122, 11122	2018-03-14 11:10:14	2018-03-14 19:10:15	2018-03-14 11:10:14	2018-03-14 16:05:29
	150.176.120.42	443	4200, 7200	2018-03-14 03:15:20	2018-04-01 19:15:19	2018-03-14 03:15:20	2018-03-14 03:15:20
	185.93.183.30	443	2144, 3122, 11122	2018-03-14 19:10:15	2018-03-14 23:10:16	2018-02-16 12:39:58	2018-03-07 11:45:48
	172.75.27.140	443	2144, 3122, 11122	2018-02-16 10:05:07	2018-02-16 11:10:06	2018-02-05 15:09:46	2018-03-07 11:44:39
	58.167.83.30	443	2144, 3122, 11122	2018-03-15 09:10:15	2018-03-20 13:10:15	2018-02-19 13:37:18	2018-03-07 11:43:34
	70.184.66.94	443	2144, 3122, 11122	2018-03-23 18:05:37	2018-03-23 21:10:14	2018-02-05 17:41:59	2018-03-07 11:43:00
	129.89.57.197	443	2144, 3122, 11122	2018-02-19 08:10:10	2018-02-19 10:10:15	2018-02-14 16:41:50	2018-03-07 11:42:07

st.	ip	port	botnet	added	removed	firstseen	lastseen
	209.151.143.34	443	2144, 3122, 11122	2018-02-16 10:05:07	2018-02-16 11:10:06	2018-02-05 16:41:09	2018-03-07 11:41:24
	155.186.105.68	443	4200, 7200	2018-03-06 10:15:17	2018-03-11 08:15:13	2018-03-06 10:15:17	2018-03-06 10:15:17
	107.185.217.40	443	23005	2018-02-16 06:20:07	2018-02-16 13:20:09	2018-02-13 03:50:14	2018-03-05 07:50:17
	186.179.99.134	443	2144, 3122, 11122	2018-03-06 22:05:43	2018-03-06 23:10:25	2018-02-27 18:37:00	2018-03-02 13:42:32
	131.104.120.60	443	2144, 3122, 11122	2018-03-06 22:05:43	2018-03-06 23:10:25	2018-02-27 19:38:27	2018-02-28 08:38:16
	12.110.252.50	443	2144, 3122, 11122	2018-02-28 23:10:20	2018-03-06 22:10:28	2018-02-14 16:42:01	2018-02-27 21:42:23
	150.176.120.43	443	4200, 7200	2018-03-06 10:15:17	2018-03-11 08:15:13	2018-02-20 12:45:26	2018-02-26 17:45:18
	2.31.131.232	443	4200, 7200	2018-03-06 10:15:17	2018-03-11 08:15:13	2018-02-16 07:45:38	2018-02-26 16:45:48
	208.58.127.110	443	23005	2018-02-16 13:20:09	2018-03-11 08:20:12	2018-02-05 16:51:17	2018-02-22 20:51:08
	46.17.3.237	443	2144, 3122, 11122	2018-02-20 02:10:10	2018-02-23 00:10:18	2018-02-20 02:10:10	2018-02-22 14:05:20
	76.94.146.77	443	2144, 3122, 11122	2018-02-16 10:05:07	2018-02-16 11:10:06	2018-02-05 16:40:37	2018-02-21 20:35:36
	73.138.14.216	443	2144, 3122, 11122	2018-02-05 15:11:22		2018-02-05 15:11:22	2018-02-21 13:39:58

st.	ip	port	botnet	added	removed	firstseen	lastseen
	23.249.164.165	443	2144, 3122, 11122	2018-03-08 01:10:28	2018-03-10 03:05:24	2018-02-16 11:35:55	2018-02-21 05:42:08
	108.188.73.120	443	23005	2018-02-16 13:20:09	2018-03-11 08:20:12	2018-02-05 15:39:45	2018-02-20 15:50:47
	73.205.129.116	443	2144, 3122, 11122	2018-02-16 19:10:07	2018-02-19 07:10:11	2018-02-14 03:43:39	2018-02-19 03:05:11
	72.240.66.196	443	2144, 3122, 11122	2018-02-05 15:06:33		2018-02-05 15:06:33	2018-02-18 18:40:16
	74.50.133.9	443	4200, 7200	2018-03-06 10:15:17	2018-03-11 08:15:13	2018-02-05 15:30:06	2018-02-17 21:46:51
	185.93.183.30	444	2144, 3122, 11122	2018-02-16 13:05:09	2018-02-17 09:44:19	2018-02-16 12:38:25	2018-02-16 14:10:08
	103.1.216.246	8443	2144, 3122, 11122	2018-02-16 10:05:07	2018-02-16 11:10:06	2018-02-16 10:05:07	2018-02-16 10:10:07
	72.196.121.198	443	4200, 7200	2018-03-06 10:15:17	2018-03-11 08:15:13	2018-02-15 20:47:14	2018-02-16 01:47:04
	108.188.147.84	443	4200, 7200	2018-03-06 10:15:17	2018-03-11 08:15:13	2018-02-15 20:47:25	2018-02-15 20:47:25
	71.190.203.72	443	2144, 3122, 11122	2018-02-16 10:05:07	2018-02-16 11:10:06	2018-02-05 16:40:48	2018-02-13 01:40:47
	45.49.124.54	443	2144, 3122, 11122	2018-02-05 15:10:50		2018-02-05 16:43:43	2018-02-08 22:43:35
	73.14.144.224	443	23005	2018-02-16 13:20:09	2018-03-11 08:20:12	2018-02-05 15:39:57	2018-02-06 09:50:56

st.	ip	port	botnet	added	removed	firstseen	lastseen
	69.75.114.66	443	4200	2018-02-05 15:29:43			
	190.208.42.36	443	4200	2018-02-05 15:30:17			
	90.45.27.34	443	3122	2018-02-05 15:11:01			
	47.22.1.187	443	2144, 3122, 11122	2018-02-05 15:10:40			
	128.83.114.21	443	2144, 3122, 11122	2018-02-05 15:11:33			
	70.182.65.230	443	3122	2018-02-05 15:11:44			
	174.76.22.140	443	23005	2018-02-05 15:39:23			
	66.63.85.26	443	3122	2018-02-05 15:11:55			
	24.236.75.22	443	10105	2018-06-07 11:37:31			
	95.150.74.40	443	4200	2018-02-05 15:29:55			
	70.184.73.157	443	2144, 3122, 11122	2018-02-05 15:06:59			
	83.152.105.116	443	3122	2018-02-05 15:08:09			

st.	ip	port	botnet	added	removed	firstseen	lastseen
	108.188.0.7	443	3122	2018-02-05 15:08:42			
	70.182.76.241	443	3122	2018-02-05 15:06:49			

Modules

Dridex uses various modules:

- The *loader* module is used to infect the client. They use an infrastructure independent from the actual Dridex operation. Loaders are not listed here, as they are mostly delivered by email.
- The *bot* module is the core of Dridex v4. It is the only module found on regular clients, apart from traces of the loader. Bots are listed in section bots.
- Supernodes and clients that are otherwise interesting to the Dridex operators (e.g., clients in corporate networks), are equipped with additional modules. For example, the *socks* module is used to redirect traffic from other infected clients, the *vnc* module is used to inspect clients before upgrading them to supernodes, or to spy on corporate machines.

The modules from the last 365 days are listed.

Bots

Dridex bots are distinguished by a version number and timestamp. For each version, there are often multiple different hashes and timestamps, which is a result of recompiling and repacking the modules.

timestamp	botnet	architecture	version	md5	v
2018-07-17 05:25:28	7200	64bit		bd99593799165161126d17cabd164460	V
2018-07-17 05:25:16	7200	32bit		b8beaa92ef68417b6f71306335529b3e	V

timestamp	botnet	architecture	version	md5	v
2018-07-16 09:22:18	7200	64bit		9bc379ffa93c47f312d17f3278624fff	\
2018-07-16 09:22:08	7200	32bit		21d41ea27f6ae652760967cb81a9216c	\
2018-06-25 14:19:46	7200	64bit		dedc619260039024df1dda42b2fbf01b	\
2018-06-25 14:19:27	7200	32bit		3c3d6fa2f3c8ad96e6f4cfd381df852c	\
2018-06-21 09:42:38	4200	64bit	4.87	a5baa566a3e9675d304e56e3cf512916	\
2018-06-21 09:42:38	7200, 11122	64bit	4.14	d00d71561128c16770349bc0241c9de4	\
2018-06-21 09:42:38	10105	64bit		cafec8ab7a6d2cffd2afdf3220a5550b	\
2018-06-21 09:42:38	3122, 23005	64bit		9a21726fdd1054098d4e75c84fde5b7f	\
2018-06-21 09:42:38	2144	64bit	4.14	724058d1cc04c3c3295bcf8d640375b1	\
2018-06-21 09:42:24	3122, 23005	32bit		f05fa10b6502a04357bd1db4fc59cd1e	\
2018-06-21 09:42:24	10105	32bit		f6ec84374c1effa56e7bf12499318c5d	\
2018-06-21 09:42:24	2144	32bit	4.14	7288dcfd23281720d7ce80925db59abe	\

timestamp	botnet	architecture	version	md5	v
2018-06-21 09:42:24	4200	32bit	4.87	4671d287f4d5f0cafbd00de50ef25510	\
2018-06-21 09:42:24	7200, 11122	32bit	4.14	8714e50aee6ed1c8a9dccc418066e0a3	\
2018-06-20 13:14:44	10105	64bit	2.25	50362d3a3b3d25985c6682cdc07dc656	\
2018-06-20 13:14:34	10105	32bit	2.25	9cff4061c873bc9bc8db8778333c094b	\
2018-06-17 11:00:18	10105	64bit	2.22	81f93600a86d319f22a5e5696ef4c92d	\
2018-06-17 11:00:00	10105	32bit	2.22	1c1b388ffcc6a971be99e3b84171d1c0	\
2018-06-15 09:01:06	4200	32bit		86afe888da74886b3f77521c383dc95a	\
2018-06-15 09:01:06	2144	32bit		2edc6e7e2c7a8968ae4cfb9d6f6f09c7	\
2018-06-15 09:01:06	7200, 11122	32bit		0adecaad257848c99178f364695562cf	\
2018-06-12 13:00:06	2144, 4200, 7200	64bit	4.14	853da33cc33197c15718ffb9220fbcaf	\
2018-06-12 13:00:06	11122	64bit	4.14	b91c009b7c2df0c98ed679e6076aead7	\
2018-06-12 12:57:00	2144, 4200, 7200, 11122	32bit	4.14	0737309e226245feecd27a35f7a50e59	\

timestamp	botnet	architecture	version	md5	v
2018-06-11 12:25:18	7200	64bit	4.87	b7e06885887b3ac39fae6e931bdf22cc	\
2018-06-11 12:25:18	11122	64bit	4.14	c49cbfdcb4fcc5096462e9f24c5d1dff	\
2018-06-11 12:25:18	2144	64bit	4.87	454f07d141e4139baeeba5bb75701bfc	\
2018-06-11 12:25:18	4200	64bit		3a0d92cfbf66a1c2d7b8af22c6008d19	\
2018-06-11 12:24:30	11122	32bit	4.14	a3a8e607a5f905928c777844e47b5f9a	\
2018-06-11 12:24:30	4200	32bit		037df38bd30a08ac4f8bff53a33070b8	\
2018-06-11 12:24:30	7200	32bit	4.87	a11c136cdc4d8a9123759980bf7aa3bb	\
2018-06-11 12:24:30	2144	32bit	4.87	1f97c1a405ceec89de6a05c8fc44a356	\
2018-06-11 09:30:25	10105	64bit	2.22	39a1d5c2e00b4dd5a9547d62bfe2f457	\
2018-06-11 09:30:11	10105	32bit	2.22	c10409766fd8f1cd80d1113b9bee4a67	\
2018-06-09 21:34:34	10105	64bit	4.14	b3c512ffa0ec2906500c70140b38a27b	\
2018-06-09 21:34:24	10105	32bit	4.14	16ddc8752e5724eff475e6c558b5c269	\
2018-06-07 14:15:20	7200	64bit	4.14	c42a6fee5b7446a087e7226d8754eb06	\
2018-06-07 14:14:34	7200	32bit	4.14	e6fc8ac7c3844e1a040e5fae6e47de7c	\
2018-06-07 12:14:07	4200	64bit	4.14	4fb3774f18c9400bd7fda15cae271e5a	\

timestamp	botnet	architecture	version	md5	v
2018-06-06 12:00:27	11122	64bit	4.86	76382ab7b72cf3e1244640ed0461c7aa	\
2018-06-06 12:00:27	4200	64bit	4.86	6f53a6a36b757eb843b81cbc82e81f34	\
2018-06-06 12:00:27	2144	64bit	4.86	fd76f3edc765e6c5971eab6c070b0963	\
2018-06-06 12:00:17	4200	32bit	4.86	bb733999c6e083528901dc29bdc966e8	\
2018-06-06 12:00:17	2144	32bit	4.86	2f5373c1244bb6d50f70952b93f3ae03	\
2018-06-06 12:00:17	11122	32bit	4.86	745bd761aaaaa56879f57d5e0cdeae9c	\
2018-06-06 10:58:14	4200, 7200	64bit	4.86	d976b6794dfb4ce442319269a642bba4	\
2018-06-06 10:58:04	4200, 7200	32bit	4.86	426af8219007ecb11ff8639b2474311d	\
2018-06-05 07:42:44	10105	64bit	2.20	641d179561c11bd2f5866247e7430475	\
2018-06-05 07:42:29	10105	32bit	2.20	747b19636ece96cc1f2b70772f71cbe3	\
2018-06-01 18:49:48	11122	64bit	4.86	f5d5af53b99ecfcc1696e943ec95a6c3	\
2018-06-01 18:49:48	2144	64bit	4.86	a65c1290917373b6ebb0543df9ca21a2	\

timestamp	botnet	architecture	version	md5	v
2018-06-01 18:49:25	2144	32bit	4.86	7b1631b97c029fc6a16fdb20a13854b7	\
2018-06-01 18:49:25	11122	32bit	4.86	f13f270b8317358f8ccb339a8c905591	\
2018-06-01 18:28:42	4200, 7200	64bit	4.86	c90e9696aa3240f154b91f70a574d26e	\
2018-06-01 18:28:04	4200, 7200	32bit	4.86	75990b40f65803028af152dacfb513a1	\
2018-05-31 12:30:36	2144, 11122	64bit	4.86	dcea2c788ca7600c1a5a9fe340f42869	\
2018-05-31 12:30:21	2144, 11122	32bit	4.86	11b78e9ee07ec42a671695487e802e0e	\
2018-05-31 12:08:30	4200, 7200	64bit	4.86	8c278fd7ef8059ef6ae7edd7acff8954	\
2018-05-31 12:08:00	4200, 7200	32bit	4.86	d7854efc87ca10aed77e77ada1015b64	\
2018-05-30 15:10:38	2144, 11122	32bit		30b4f2c39803220f1712529c07186924	\
2018-05-30 14:40:32	4200, 7200	32bit		c32270515d30840b42445e5ff64e97a9	\
2018-05-30 12:17:53	11122	64bit	4.86	5cb82acf05b86fe16953ff4a1c412a97	\
2018-05-30 12:17:53	2144	64bit	4.86	ba6d916e590e037596aef06bf09d5796	\

timestamp	botnet	architecture	version	md5	v
2018-05-30 11:11:22	7200	64bit	4.86	e499b41403337ae51cb2a7c23b14e175	\
2018-05-30 11:11:22	4200	64bit	4.86	34488bd593341ca9f1c097f5e7d16e1b	\
2018-05-29 11:40:10	2144, 11122	64bit	4.86	4faf563dad4c18854c416562fe6cf6a1	\
2018-05-29 11:39:42	2144, 11122	32bit	4.86	6650a83efe4719129cac32f06e8765c2	\
2018-05-29 10:20:33	4200, 7200	64bit	4.86	9f138ef68f86abadf9f78602083f79bb	\
2018-05-29 10:19:55	4200, 7200	32bit	4.86	5d087ecef12ed735a4f22324cbfc3d70	\
2018-05-28 10:07:56	4200	64bit	4.86	b5a7401a29ca860ed128f9f1ad4aaecd	\
2018-05-28 10:07:56	7200	64bit	4.86	c2edb307a55b8664b5c7e3f2745d9d64	\
2018-05-28 10:07:38	4200, 7200	32bit	4.86	3e3668b0419a5dabaa55b073a3bf4ec5	\
2018-05-25 13:38:13	2144, 11122	64bit	4.86	fa54d7c3e7740385cdb1d286e29a598e	\
2018-05-25 13:37:53	2144, 11122	32bit	4.86	70d84ec4cde6323bdce3273870970aba	\
2018-05-01 14:43:04	2144, 3122	64bit	4.85	e7172aadda00497ce11527fe0153132c	\

timestamp	botnet	architecture	version	md5	v
2018-05-01 14:43:04	11122	64bit	4.85	7d4ffad425e9cc91c60d817ba42f2c55	\
2018-05-01 14:42:31	11122	32bit	4.85	5c0904e7ede84040e3b1f172e4892c31	\
2018-05-01 14:42:31	2144, 3122	32bit	4.85	f71ea8289672e4358fff0c5113b97b81	\
2018-04-27 15:22:59	3122	64bit	4.85	3faa10d75f57d08e4945bcfed2cc036d	\
2018-04-27 15:22:59	2144	64bit	4.85	d909405643ee63f045b9a38695564536	\
2018-04-27 15:22:59	11122	64bit	4.85	507596b2d517678183717c4e682be03d	\
2018-04-27 15:22:32	11122	32bit	4.85	a73472db9c92acf93a9ee96e3335912b	\
2018-04-27 15:22:32	2144	32bit	4.85	1048b874e0896a0c3d298f431769668c	\
2018-04-27 15:22:32	3122	32bit	4.85	08876dbf3845e12e419cbfb9cc99f5cf	\
2018-03-23 18:14:53	2144, 3122	64bit	4.85	033d7486b43935a8adf5796835d088d4	\
2018-03-23 18:14:53	11122	64bit	4.85	b2555356e1695a975b8fbd75d1be73ac	\
2018-03-23 18:14:41	2144, 3122	32bit	4.85	de6425b9b266455b8009129085f99117	\

timestamp	botnet	architecture	version	md5	v
2018-03-23 18:14:41	11122	32bit	4.85	5bb318f28821576e3975b13b9eebf617	\
2018-03-23 18:13:54	23005	64bit	4.85	ceeb0c36d1eeb5f35f82ddd3bce58716	\
2018-03-23 18:13:27	23005	32bit	4.85	d819d6785b313258f4434b5e3db7b268	\
2018-03-20 09:35:23	2144	64bit	4.85	cc8ab8cafcd225ed4ebc70e0139b6890	\
2018-03-20 09:35:23	3122	64bit	4.85	a8d7b2014fa44252967635c15f8cab50	\
2018-03-20 09:33:41	2144	32bit	4.85	3eade9e5b3dbdfdd2bd16571be498fd3	\
2018-03-20 09:33:41	3122	32bit	4.85	e755a16547585be1e7338762828c88f0	\
2018-03-14 21:36:57	2144	64bit	4.85	271543a2e8ecb8d5fe9abf73441a982e	\
2018-03-14 21:36:57	2144, 3122	64bit	4.85	7ee2fbfee2623de1bc5b7ae3a0633891	\
2018-03-14 21:36:42	2144, 3122	32bit	4.85	879d3069145d6276f2a1cb8135f4078a	\
2018-03-14 21:36:42	2144	32bit	4.85	a4aad924d78d7070831ec5695f19dc78	\
2018-03-11 07:48:28	23005	64bit	4.85	df80d463f19b61f2bc10622e2172fd36	\
2018-03-11 07:48:28	23005	64bit	4.85	f41fb1019007c5e03ff3d38ee91523dd	\

timestamp	botnet	architecture	version	md5	v
2018-03-11 07:48:14	23005	32bit	4.85	306b584f2b6189699b9597a14734fa95	\
2018-03-11 07:48:14	23005	32bit	4.85	3113f7ca01b174211eae1a3a8f1614df	\
2018-03-11 07:45:56	2144, 3122	64bit	4.85	8d26bc42ba1906fefe4c4f63c4b0802e	\
2018-03-11 07:45:42	2144, 3122	32bit	4.85	537d5a22641f4816bb566cb505d084f6	\
2018-03-11 07:22:01	7200	64bit	4.85	123ca5b9d0858aa5e67c79f483ec1cea	\
2018-03-11 07:22:01	4200	64bit	4.85	e12b7bbb65aa0b1c1d63c3ebd59ad115	\
2018-03-11 07:22:01	4200	64bit	4.85	bc303564876fb407642032cf93a93058	\
2018-03-11 07:21:42	4200	32bit	4.85	b773caf389f2da2e4aeadc1f9fd69b2a	\
2018-03-11 07:21:42	7200	32bit	4.85	4e29341b39d1f32e50546a8ac2ac8871	\
2018-03-11 07:21:42	4200	32bit	4.85	93bfdb5b9810387f1769a6f76461f550	\
2018-03-06 22:04:42	2144, 3122	64bit	4.85	ba9472537e6404849dddf9341d155928	\
2018-03-06 22:04:31	2144, 3122	32bit	4.85	6b68cb8768d8c6a0badcd1bbdafb8af7	\
2018-03-06 10:05:33	4200	64bit	4.85	0a4ef87b5ab1593121f3e3cfad9ea476	\
2018-03-06 10:05:22	4200	32bit	4.85	85d3adf228524bb7bc6ea66d12ef18cd	\
2018-02-27 09:23:53	2144, 3122	64bit	4.85	6d3b2c5ee970e7c37d24dce9d9f70666	\

timestamp	botnet	architecture	version	md5	v
2018-02-27 09:23:39	2144, 3122	32bit	4.85	32b2e94cb2f7d4a71123b4f9585c63b3	\
2018-02-20 13:02:42	4200	64bit	4.85	7ca54a11bf979832c19000d53874bb23	\
2018-02-20 13:02:28	4200	32bit	4.85	876fa2bab0a90e8d84045f71bb84f734	\
2018-02-19 06:53:59	2144, 3122	64bit	4.85	b23a9bd3ee31af8b78d18bb92e7f2257	\
2018-02-19 06:53:37	2144, 3122	32bit	4.85	353053924fb970d00e3ad897eeaa1ff5	\
2018-02-16 07:13:10	23005	64bit	4.83	d053911bbc6865377eb70720aa4c4d4d	\
2018-02-16 07:12:54	23005	32bit	4.83	964e6212ab22e166a343f5417514f62d	\
2018-02-16 07:10:56	4200	64bit	4.83	4796d47eb1ae2c03c98d31c4bb9e7327	\
2018-02-16 07:10:44	4200	32bit	4.83	66034294e67c0465453fc080b22ae76a	\
2018-02-16 07:07:38	2144, 3122	64bit	4.83	491cb5e246e51c01d30840ce75a7a8fb	\
2018-02-16 07:07:06	2144, 3122	32bit	4.83	7c7d957fcd93ef3d1b78054aa2fb4472	\
2018-02-15 15:18:43	4200	64bit	4.82	a889fc46b4eed4a031343706ea731157	\

timestamp	botnet	architecture	version	md5	v
2018-02-15 15:18:22	4200	32bit	4.82	8bc3faf395280ce664c21bff1e019959	\
2018-02-14 09:17:49	2144, 3122	64bit	4.82	2ef3236e531301a52756d262c7a3249f	\
2018-02-14 09:16:41	2144, 3122	32bit	4.82	70b71d97bcd65b27c7e6f44797672318	\
2018-02-05 09:28:13	2144, 3122	64bit	4.82	011687661ecc9673141e8ffafb7004af	\
2018-02-05 09:27:42	2144, 3122	32bit	4.82	94fd7c297e7ddc4dc2ba51af095685d0	\
2018-02-05 09:24:10	23005	64bit	4.82	32ac659d0f4233bc4bf98ada3f550406	\
2018-02-05 09:23:23	23005	32bit	4.82	3fa18db246e3766ca221858e44d4a0fc	\
2018-02-05 08:48:40	4200	64bit	4.82	3f7155b3a742fdf5d8539ec384090510	\
2018-02-05 08:48:30	4200	32bit	4.82	1677932806f6cad5af01fa3a58bed742	\
2018-01-18 13:04:13	2144, 3122	64bit	4.80	1264dbcf9106b7adab3682b9b42bdfcf	\
2018-01-18 13:04:02	2144, 3122	32bit	4.80	a40ba82daea1dce261b2231d2eb8fd70	\
2018-01-09 20:01:21	2144, 3122	64bit	4.80	2967e39fe0b22f020489028f159c620b	\

timestamp	botnet	architecture	version	md5	v
2018-01-09 20:01:07	2144, 3122	32bit	4.80	e0b43753cf06c3ccd65c9e5b54fb74ee	\
2017-12-22 22:29:34	2144, 3122	64bit	4.80	f441b8d2f70ef84e8cc71556f293ff7a	\
2017-12-22 22:29:19	2144, 3122	32bit	4.80	44d7924d72eb125d71d194415f585016	\
2017-12-16 13:23:00	2144, 3122	64bit	4.80	cffb11367fa1833d4b8fd74fc3b48f06	\
2017-12-16 13:22:48	2144, 3122	32bit	4.80	063ef17c48eae1c326e6cd97364e5f9f	\
2017-12-08 20:44:40	2144, 3122	64bit	4.77	fa593738687c4de41562e962fb4ca9c1	\
2017-12-08 20:44:29	2144, 3122	32bit	4.77	edba64cb2157ddb77cb33cc428a48076	\
2017-12-04 07:37:53	2144, 3122	64bit	4.75	dcf43e6642171ac71b4664846636e5dd	\
2017-12-04 07:37:40	2144, 3122	32bit	4.75	f93155d82bdbdd513f93106240b35b17	\
2017-11-25 13:14:49	2144, 3122	64bit	4.74	2415a6f409c9572f7eda4ba789359c56	\
2017-11-25 13:14:38	2144, 3122	32bit	4.74	ed570695236713a847a81fb62e54f782	\
2017-11-21 13:52:04	2144, 3122	64bit	4.74	a0e62320c474e6df73fc032686e6c97e	\
2017-11-21 13:51:49	2144, 3122	32bit	4.74	d25709b54bb78ed8e34652bf23072dae	\
2017-11-16 15:02:36	2144, 3122	64bit	4.73	213861f6c38cf79771a4cc136474bf67	\

timestamp	botnet	architecture	version	md5	v
2017-11-16 15:02:24	2144, 3122	32bit	4.73	ba191e35a260f6d106ccbe82a10aa5cc	\
2017-11-16 10:49:31	2144, 3122	64bit	4.72	eeace3e72424b8c3592bca8ecb32555d	\
2017-11-16 10:49:17	2144, 3122	32bit	4.72	1dcfab5e9a43ce0320bf05e2bed0e8f3	\
2017-11-08 12:31:23	2144, 3122	64bit	4.71	ec58af9975f6322fbe54ef8861c4ab25	\
2017-11-08 12:31:10	2144, 3122	32bit	4.71	b6321435318466353052 1e41f1452078	\
2017-10-30 07:04:49	2144, 3122	64bit	4.68	81135fa4b14a33cdbda15ebc1ec58294	\
2017-10-30 07:04:31	2144, 3122	32bit	4.68	ad343e1aa8fb15c5cf04dd817fd3a1dd	\
2017-10-24 05:15:49	2144, 3122	64bit	4.68	996c8c52b5aa9626cbbff991d86ced57	\
2017-10-24 05:15:11	2144, 3122	32bit	4.68	6683059357268d4a28ea8f4adb587ef5	\
2017-10-20 15:55:07	2144, 3122	64bit	4.68	4e6c207f0f069934b8da7fa48c235a44	\
2017-10-20 15:54:32	2144, 3122	32bit	4.68	ce82508dece9d26ce3fb84ea826a9eff	\
2017-10-18 11:34:02	2144, 3122	64bit	4.68	a0de22f3b01556deeae2c90a690b5845	\
2017-10-18 11:33:35	2144, 3122	32bit	4.68	2a02912728b77f6a5cc57812dac7be62	\
2017-10-12 23:32:10	2144, 3122	64bit	4.67	d957cda6190e8e04e7ed6d3cb8f79326	\

timestamp	botnet	architecture	version	md5	v
2017-10-12 23:31:56	2144, 3122	32bit	4.67	bf91a9159929614de2f9dc95c59de516	\
2017-10-02 22:23:23	2144, 3122	64bit	4.67	0caaae681f61ba974bd5d4a013312ee2	\
2017-10-02 22:19:39	2144, 3122	32bit	4.67	58692ccca8e32b7c7f48e76be001bfa0	\
2017-09-18 05:13:14	2144, 3122	64bit	4.66	d8c6f5d7d60a8c10fe1773c50d426079	\
2017-09-18 05:13:00	2144, 3122	32bit	4.66	8cfa2bc7ce6cc76fb7252392d29e9a21	\
2017-09-10 16:17:45	2144, 3122	64bit	4.66	303299aca690f1d5de966b542c89e10f	\
2017-09-10 16:17:16	2144, 3122	32bit	4.66	4823da9b1fa44bf06b5a1dfcf52ee03e	\
2017-09-04 18:29:51	2144, 3122	64bit	4.65	8319f4b39bd607041bc71e6b748fb533	\
2017-09-04 18:28:42	2144, 3122	32bit	4.65	8deb67a267969ce49f87cc3623849507	\
2017-08-27 11:14:58	2144, 3122	64bit	4.65	d0436a7e50f39e42f00eee73a9ba7be6	\
2017-08-27 11:13:34	2144, 3122	32bit	4.65	f520c0c589a255df597f240c37837f81	\
2017-08-20 16:03:51	2144, 3122	64bit	4.62	3df2e31681a7e529139a9fed7f733ad6	\

timestamp	botnet	architecture	version	md5	v
2017-08-20 16:03:41	2144, 3122	32bit	4.62	56152d48f52c337e2348c75254f142db	\
2017-08-12 22:22:06	2144, 3122	64bit	4.62	20cb606139fa6f13b87b32997dc5aa95	\
2017-08-12 22:21:54	2144, 3122	32bit	4.62	a05c5b9f11453fc8090e2d2d9d73d4c0	\
2017-08-03 20:33:08	2144, 3122	64bit	4.62	67290af5a4d60537720e54a4fc6b4d97	\
2017-08-03 20:32:06	2144, 3122	32bit	4.62	5705837474d6126e8e0781b1656e7415	\
2017-07-31 21:36:25	2144, 3122	64bit	4.61	b62d54c8bd2c2d6b6b2a6cf81b0fb097	\
2017-07-31 21:36:04	2144, 3122	32bit	4.61	14aa615a9be3edc86e12f6fa6ac0b154	\
2017-07-25 16:30:40	2144, 3122	32bit	4.61	0f676b95ae81e27ae286194fc2c90fb6	\
2017-07-25 16:27:55	2144, 3122	64bit	4.61	1fbbcd16d07fa55c40db393e0916dd1c	\

Auxiliary Modules

The auxiliary modules are often off-the-shelf, legitimate binaries (e.g., VNC or the socks proxy). These modules are updated much less frequently than Dridex bots.

Dridex v4 uses CRC32 checksum in lieu of names. In some instance, the names behind the CRC checksums are known. In other cases, the names are missing. In these cases only the CRC32 checksum is shown.

timestamp	name	botnet	architecture	md5	viru
2018-06-01 15:06:13	vnc	4200, 7200	64bit	4bf8d67b5b98d03cf6318491586fe3a2	VT
2018-06-01 15:06:06	vnc	4200, 7200	32bit	d89722941c45005ad5cc33fd48fe48ec	VT
2018-05-29 10:58:26	vnc	10105	64bit	8d822468eade205b2b2a036ea9f33239	VT
2018-05-29 10:58:17	vnc	10105	32bit	4d0b5e5a518fdadd4b5924e5a1dead5f	VT
2018-05-18 13:56:08	socks	2144, 3122, 4200, 7200, 10105, 11122, 23005	64bit	a87eaba1b46ea8a99b0f4710777c013b	VT
2018-05-18 13:56:01	socks	2144, 3122, 4200, 7200, 10105, 11122, 23005	32bit	a6fb408a4ee7efe45299d2c531234093	VT
2018-05-18 13:55:55	vnc	2144, 3122, 4200, 7200, 10105, 11122, 23005	64bit	ec0a15c4bcfe7377c5bed3d37cc25bd0	VT
2018-05-18 13:55:47	vnc	2144, 3122, 4200, 7200, 10105, 11122, 23005	32bit	4e875d224503eb68f9dc40dc28a0a754	VT

timestamp	name	botnet	architecture	md5	viru
2018-02-16 07:11:18	vnc	4200, 7200	64bit	c63af594f1ca740e2b57d0bd4eead601	VT
2018-02-16 07:11:13	vnc	4200, 7200	32bit	67feb77f8a0958a12655765ef9744c86	VT
2018-02-15 19:28:44	vnc	23005	64bit	9e2dcff64c9c000b06dd327b5838b885	VT
2018-02-15 19:28:31	vnc	23005	32bit	1cf32534fe2bcd55420301fe18a1dfc1	VT
2018-02-15 19:27:11	vnc	2144, 3122, 11122	64bit	4a0b19b2a6ccad8491f9692bc4429b9a	VT
2018-02-15 19:27:03	vnc	2144, 3122, 11122	32bit	a449cce578a68550c19b9f29de7872f3	VT
2018-02-07 12:52:45	vnc	2144, 3122	64bit	b29c9c88b52693213303c6d0364442ee	VT
2018-02-07 12:52:23	vnc	2144, 3122	32bit	1cedc79b60dedbf9462279027a9a575c	VT
2018-01-29 14:44:07	vnc	23005	64bit	fde741f87afd2dbf3babce86b2abc55f	VT
2018-01-29 14:43:57	vnc	23005	32bit	8c70d12fe79a6860b2ef28de45aa201c	VT
2018-01-28 13:08:30	n/a	23005	32bit	88ffbfb96c645904f1f7ec3336bbaa01	VT
2018-01-28 13:07:40	n/a	23005	64bit	f501fe0bb0dd2816d4107ba11fcb136b	VT

timestamp	name	botnet	architecture	md5	viru
2018-01-28 13:01:20	socks	23005	64bit	55550b908499159083986fc0678a1c2c	VT
2018-01-28 13:01:16	socks	23005	32bit	dc80969ec4f3a778e3b32da1b42daebb	VT
2017-12-30 23:01:35	n/a	2144, 3122, 11122	64bit	937a7ba06ed92aee14e11c457a11e322	VT
2017-12-30 23:01:28	n/a	2144, 3122, 11122	32bit	c39d8295ce6d81c57e7f3044b5feeaae	VT
2017-12-27 15:32:56	n/a	4200	32bit	97cf4507315546c5105db08e017f2412	VT
2017-11-08 12:35:48	n/a	2144, 3122	64bit	d99113d6a87989570fa95b03df0415ee	VT
2017-11-08 12:35:43	n/a	2144, 3122	32bit	3022b146b34dde5f81e8eaf46c22e046	VT