Top100 恶意程序样本特征

序号	MD5	类型
1	aed57cab3e622e3a52f0f1f1b8da9bc7	蠕虫
2	daca5c158c6a765ce8ec67d5b079bcf5	木马后门
3	3d2a33a471932a78bf807ba532d5a279	感染性病毒
4	003204036798a24f6f9941c08b3ed9e4	感染性病毒
5	19f92fb54e1fb740d847ba4555fe107e	木马
6	aa90dc46799ef6c27f4192711f414935	脚本恶意文件
7	027173d7337ce8d6db3e2133889c5113	木马
8	f1dae8ee2997ca8018efd439c99ce3bc	脚本恶意文件
9	19dd39bdb17a4a78801a14b070148163	蠕虫
10	324af2abc1f3aef92eb6fd596b6eaa00	蠕虫
11	5f973c8004be579518a85dfe2bcd56d7	蠕虫
12	6cb14af389115a1d065bff5ba6cc92c0	木马后门
13	eca1a1c6c3524896a787a95615935d46	木马后门
14	31b423c1071d4abe452854d08bc1e650	木马后门
15	4a43ea617017d5de7d93eb2380634eee	木马后门
16	2c0caac60fa30880ba7ffb50d726be24	木马
17	e2d2b93ad30ffaa5a1dd19ecc3957f80	木马后门
18	3b8c834fba091029b515cfb4edf197f0	木马
19	5660c4b61afede1f9781aea985bff3b0	感染性病毒
20	afff5145f0ac01e4e62975223ad5b240	蠕虫
21	18484fb0c3817656338d9bb3952f16af	木马
22	0482ee1c7011e1957f51155840ebc61e	蠕虫
23	b622474b7ca562f6ccc83692fc4af743	感染性病毒
24	c522a47c1f40e10e0718f17f9d31819d	木马
25	9394752b5e59f5eceacb9a53af9a0348	蠕虫
26	703083bfddf904e23709948f92545c36	木马后门
27	dca37d994a239faf332181d8a22d4b71	木马后门
28	23355a2c17345954e2bbaa30a10a0788	木马后门
29	44377db91d99e4bcf825f6fb7ccfd6bf	木马
30	f08518391709f705402d1f379bdcfd2c	木马
31	65be416f75e513e06151cda59fbc9d9c	蠕虫
32	e7fb6003e3023f7ce5afce2e65fec4e6	木马
33	1a78901210508c252080ac22f697c9ce	木马

34	56e9e121d68b5631a360d56b2ef4777f	木马
35	457d2248b6c5f86297849dfbc611e423	蠕虫
36	e4c2657348b2c81cf280c3710e2afaf9	蠕虫
37	7142214611 6a6fbf27cc3a9f0afd13d7	木马
38	d6e8e6fbbbdb3d7783719df2823b02fd	蠕虫
39	080d8ef2430b49f991b460abf4af5156	蠕虫
40	8f98eb277e1dcb4b8941982c2512dfb7	僵尸网络
41	e1028e576a1769d44de70ddc2eb13c98	木马后门
42	2db461d2eed7283edac289de41fd2ecc	木马
43	adaec7cb0e88e13f31081072d811354b	木马
44	94fef1eebf8b9ea06f49d7f8b7814826	木马后门
45	ea056490147d9154343cabf79ee9f096	木马
46	0a456ffff1d3fd522457c187ebcf41e4	蠕虫
47	b460ff68f446ad6dbe96a8b5efb37ce8	木马
48	38888c3be03310142ad8513e5d7ead00	木马后门
49	bd8cb75cd1d80a311d72db68b7bde770	木马后门
50	97639ff88edd3d74f211d3f279b3792b	木马后门
51	d91814499380778db278535d8c4f7ac7	木马
52	5c5559e1ace88531b0403b61216ef235	木马
53	b739969c0d1b3aeb2c73779708123a94	木马后门
54	99063801d8185450658859547a533e79	木马
55	9d518882e451d2c343f6b17e0ef5fd0d	木马
56	9536411fdb06e67549088120517d36a2	木马
57	d2b777a93719e548d0baf4c886e124d3	僵尸网络
58	9a125df5a4a57ca63182c4f0cd9c398b	木马
59	cee0d7092ec83373078d0045a0c74c40	木马后门
60	27bc4c432399f27d1a0ccfde912e511f	木马
61	5e4d7a6cd987047b0c5e219649bfacc1	木马
62	5ae16ed25d9193c6dea13cfc6dd74592	木马后门
63	5ecc511f7234bade713524ce63eb9683	木马
64	d31e46536434b776a7b84b24e7f7bad2	木马后门
65	69ff0b34c72798baa5eb23b3b022e7bc	木马后门
66	cf3a6761cb8d9433052751e0458bfdc2	感染性病毒
67	44b414247bf30b878ba0aaa3e59067b7	木马
68	f9a3e3ad052aece41ef2d71973c61ef9	木马
69	e3a8a2442bc441d5d732d42deeb3b75d	木马
70	5f855b18f8b30acaf2e9764e99fea3a3	木马
71	0726358ac00ad2754b2afe95026890b1	感染性病毒
72	d98324bfb8412f4e282bbb3e79fb8eea	木马

73	dc26d60e5c21f34f09c73f34464672e4	木马
74	d1319e42cce1ee0079c2a0e09c24c79b	木马
75	ff06ef977e0fbfd2ca28ac9cf75325ce	木马
76	c055f0613659385848ebd99c073495ec	感染性病毒
77	dce19327242a78c2dcbe0103cbe501cb	僵尸网络
78	e9703de3e8df1f1775caf4b80a3a2197	脚本恶意文件
79	1190bbb0949a2e7a5354d5521dde18d4	木马
80	aac9bc7fd2ed52d277199ccf373a996f	挖矿软件
81	fbff63ea2cf4421f5dff8542dd0bdc0d	感染性病毒
82	1e30930395b164f7efd59a3e48707166	病毒
83	262440d08b496299927e474e38e2f9a5	病毒
84	6d69be00f87b765e1cf5c7303a2f4cd6	蠕虫
85	22d079fe899222446fc9e0b6a49f4692	木马后门
86	e5f7f3604ab2d261d90560664cb241b2	木马后门
87	bdee7b3094cb90041334ab63515f4629	木马
88	e19c7a0549d03e1e7aff28a795f70744	脚本恶意文件
89	7522449b6cef79acc7cce1cd5a675367	木马
90	59f45462df60aade07ba0bfc4a2f3529	木马
91	a7027359c127c41f595e192d5bc6f93c	感染性病毒
92	d53cf8b5e4443a767a00c915c62cbddb	木马
93	92babcca187ea582599c4c750018887d	木马
94	2e04cdcc54ff9da1e8b8718009a808c9	病毒
95	6adb5eca53d013655a59383c4cf1ec53	木马
96	f0794e1f9d94cb658447f976cca2074f	病毒
97	2120131ba9b71c39e76762c0326334ba	木马
98	44114b98d90f8bfc9e18c285937ca092	木马
99	f0669c3773be16aaaf0165899be9cd89	木马
100	5c7b75b53828d1efe56126a7b0e8e005	木马后门

Top100 异常流量特征

序号	IoC	类型
1	ii.haqo.net	勒索
2	pp.abbny.com	木马（内核、远控、银行、脚本、后门）
3	oo.beahh.com	木马（内核、远控、银行、脚本、后门）
4	v.beahh.com	僵尸网络
5	da.testiu.com	木马（内核、远控、银行、脚本、后门）
6	i.haqo.net	挖矿
7	p.abbny.com	僵尸网络
8	o.beahh.com	勒索
9	xred.mooo.com	木马（内核、远控、银行、脚本、后门）
10	c.najwahaifamelema86.com	木马（内核、远控、银行、脚本、后门）
11	c.najwahaifamelema87.com	木马（内核、远控、银行、脚本、后门）
12	c.najwahaifamelema88.com	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
13	c.najwahaifamelema89.com	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
14	c.najwahaifamelema100.com	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
15	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwff.com	勒索
16	c.najwahaifamelema50.com	木马（内核、远控、银行、脚本、后门）
17	c.najwahaifamelema36.com	僵尸网络
18	c.najwahaifamelema53.com	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
19	db.testyk.com	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
20	apps.identrust.com/roots/dstrootcax3.p7c	木马（内核、远控、银行、脚本、后门）
21	c.najwahaifamelema48.com	木马（内核、远控、银行、脚本、后门）
22	a.najwahaifamelema1.com	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）

23	a.najwahaifamelema12.com	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
24	a.najwahaifamelema5.com	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
25	a.najwahaifamelema49.com	僵尸网络
26	a.najwahaifamelema4.com	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
27	a.najwahaifamelema6.com	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
28	a.najwahaifamelema38.com	僵尸网络
29	a.najwahaifamelema50.com	木马（内核、远控、银行、脚本、后门）
30	a.najwahaifamelema36.com	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
31	a.najwahaifamelema54.com	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
32	a.najwahaifamelema51.com	僵尸网络
33	orzdwjtvmein.in	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
34	somicrososoft.ru	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
35	ftp.byethost10.com	其他
36	anam0rph.su	木马（内核、远控、银行、脚本、后门）
37	ygiudewsqhct.in	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
38	bdcrqgonzmwuehky.nl	木马（内核、远控、银行、脚本、后门）
39	xdqzpbcgrvkj.ru	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
40	johnhop77.ddns.net	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
41	s.albrrualt.ru	木马（内核、远控、银行、脚本、后门）
42	s.yvjznwcnk.ru	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）

43	s.zltuxtlsr.ru	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
44	s.owsqcjijt.ru	木马（内核、远控、银行、脚本、后门）
45	s.czszjaijy.ru	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
46	s.ijrjnpnzj.ru	木马（内核、远控、银行、脚本、后门）
47	s.omwsgcjzr.ru	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
48	s.eiwmqmkjl.ru	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
49	s.lnfwfygux.ru	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
50	s.tjpuxuwrg.ru	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
51	webmine.cz	挖矿
52	s.etrszktqr.ru	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
53	s.yfsamwekj.com	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
54	s.isolohxyr.ru	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
55	s.ohahctehc.com	木马（内核、远控、银行、脚本、后门）
56	s.vkpjlqvhp.ru	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
57	s.trxspgpzz.ru	木马（内核、远控、银行、脚本、后门）
58	www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com	其他
59	z.totonm.com	木马（内核、远控、银行、脚本、后门）
60	s6_rep.listw.top	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）
61	s.uusgbprgo.ru	木马（内核、远控、银行、脚本、后门）
62	du.testjj.com	僵尸网络
63	s6_down.listw.top	黑灰产（流氓推广、恶意软件、恶意下载、博彩、色情等）

64	c.so1aa00.com	木马（内核、远控、银行、脚本、后门）
65	c.najwahaifamelema38.com	木马（内核、远控、银行、脚本、后门）
66	c.roooggeyyy4.com	木马（内核、远控、银行、脚本、后门）
67	c.eire5bobohayawen42.com	木马（内核、远控、银行、脚本、后门）
68	c.najwahaifamelema99.com	木马（内核、远控、银行、脚本、后门）
69	c.najwahaifamelema47.com	木马（内核、远控、银行、脚本、后门）
70	c.najwahaifamelema32.com	木马（内核、远控、银行、脚本、后门）
71	c.zabrak0vmin0kov2.com	木马（内核、远控、银行、脚本、后门）
72	c.najwahaifamelema98.com	木马（内核、远控、银行、脚本、后门）
73	c.najwahaifamelema51.com	其他
74	c.zabrak0vmin0kov1.com	其他
75	survey-smiles.com	木马（内核、远控、银行、脚本、后门）
76	c.najwahaifamelema49.com	木马（内核、远控、银行、脚本、后门）
77	coco.miniast.com	挖矿
78	c.zabrak0vmin0kov4.com	其他
79	c.zabrak0vmin0kov5.com	其他
80	iron.tenchier.com	挖矿
81	log.miniast.com	其他
82	ball.hamturer.com	僵尸网络
83	s.txrtobevg.ru	木马（内核、远控、银行、脚本、后门）
84	see.ornamen.tk	挖矿
85	gus.achtlemon.com	僵尸网络
86	trt10.t3tgz.com	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
87	amnsreiuojy.ru	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
88	v1.fpzskbc.ru	木马（内核、远控、银行、脚本、后门）
89	www.downxia.com	木马（内核、远控、银行、脚本、后门）

90	api.jm.taolop.com	木马（内核、远控、银行、脚本、后门）
91	bit.ly	木马（内核、远控、银行、脚本、后门）
92	v1.dtisylr.ru	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
93	fget-career.com	僵尸网络
94	pro.csocools.com	挖矿
95	v1.lbjcwix.ru	僵尸网络
96	v1.nlrkwrsc.net	木马（内核、远控、银行、脚本、后门）
97	donate.v2.xmrig.com	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）
98	v1.xjnpziz.com	木马（内核、远控、银行、脚本、后门）
99	v1.qtlmzqwq.com	木马（内核、远控、银行、脚本、后门）
100	ilo.brenz.pl	病毒（宏病毒、恶意病毒、感染型病毒、蠕虫病毒、通用病毒）