

保险业安全值报告

（2016 第一季度）



www.aqzhi.com

2016. 5

报告概述

安全值行业报告是基于威胁情报数据，利用大数据的分析方法对行业整体安全状态进行评价和分析，本报告对保险业中 105 家保险公司进行安全评价和量化风险分析。

本报告是针对各保险公司的数据信息进行采集，共计 105 家公司的安全值进行分析，并从业务安全、隐私安全、应用安全、主机安全、网络安全、环境安全 6 个维度进行风险量化分析。

通过安全值对行业第一季度的数据分析发现：

根据 2016-5-11 安全值数据，保险业安全值为 853，整体评价为“**一般**”。共 105 个公司，其中 65 家（62%）评价为“**良好**”；35 家（33%）评价为“**一般**”；5 家（5%）评价为“**较差**”。

应用安全、隐私安全和网络安全问题较为严重，三类风险中 61 家（58%）保险公司存在应用安全问题；103 家（98%）公司存在隐私安全问题；

105 家保险公司中有 31 家机构（30%）遭受到 DDOS 攻击，构成了网络安全威胁的主要问题。近 90 天内共发现 1346 次 DDOS 攻击记录，影响到 32 个 IP 地址，8081 和 443 端口受到攻击最多。攻击源地址共 69 个，通过在全球黑名单中进行查询，发现 17 个是黑名单地址，为较高威胁的攻击源地址，行业用户应进行监控，并采取控制措施，报告第 4 章将进行详细分析。

风险指标说明

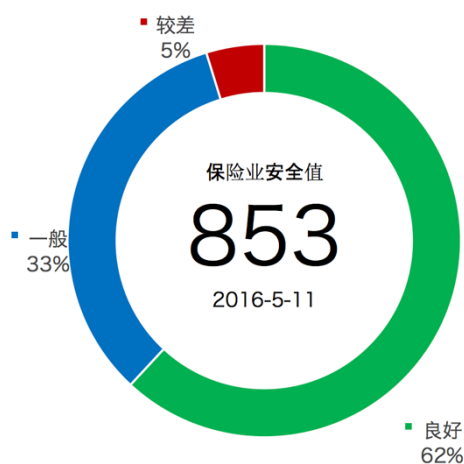
安全值根据外部大数据和威胁情报数据进行挖掘，建立并持续更新指标体系，当前由 12 项安全风险指标支撑安全评价和分析。

- 域名劫持 域名解析异常，部分用户数据可能被非法劫持。
- 域名被封 域名被判定为不可信任的域名，部分用户可能无法访问
- 邮箱被封 邮件地址被认为垃圾邮件域，发出的邮件可能被认为垃圾邮件
- IP 被封 IP 被判定为恶意地址，可能影响网络正常通讯
- 漏洞披露 在互联网安全社区上披露了系统的安全漏洞
- Web 攻击 在线 Web 系统遭受了黑客的 Web 攻击或扫描
- 域名信息泄露 域名未做隐私保护，域名管理员可能会遭受钓鱼攻击
- 帐号信息泄露 企业的员工帐号在第三方数据库中被泄露，可能包括密码等敏感信息
- 恶意代码 信息系统上发现后门、病毒、木马等恶意代码
- 僵尸网络 网络内的主机可能已经被入侵，并植入木马、后门程序
- 异常流量 在线系统或网络遭受 DDOS 拒绝服务攻击
- 公有云风险 您正在与恶意网站共用同一个云服务资源

目录

报告概述.....	2
风险指标说明.....	3
1. 行业总体概况.....	5
1.1. 总体安全值分布.....	5
1.2. 互联网资产统计.....	5
2. 风险分布及量化评估.....	6
3. 风险指标分析.....	7
4. 异常流量风险详细分析.....	7
附表：保险公司名单（字母排序，不分先后）.....	10

1. 行业总体概况



根据 2016-5-11 安全值数据，保险业安全值为 853，整体评价为“一般”。共 105 家公司，其中 65 家（62%）评价为“良好”；35 家（33%）评价为“一般”；5 家（5%）评价为“较差”。

评价	得分范围	单位数量	占比
良好	901-1000	65	62%
一般	601-900	35	33%
较差	400-600	5	5%

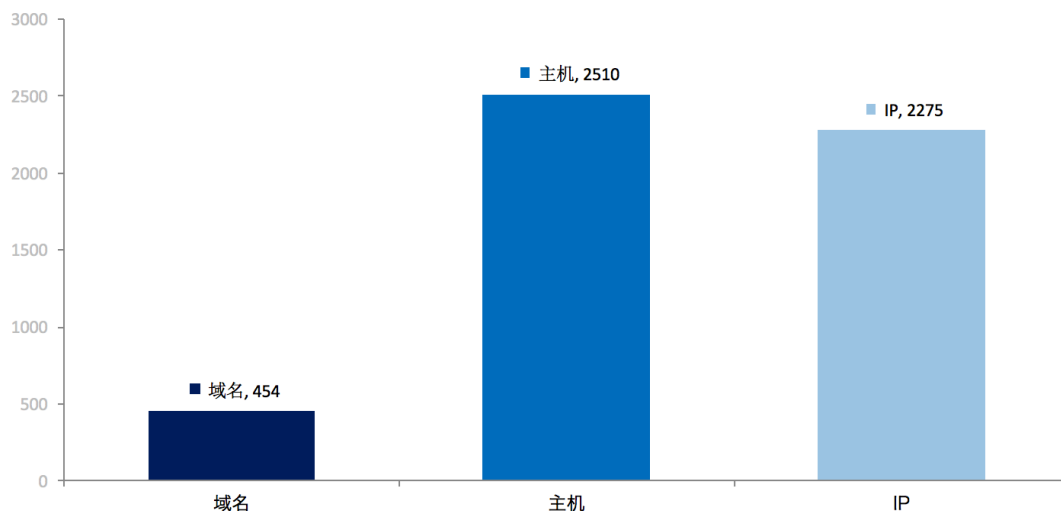
1.1. 总体安全值分布



从安全值的分布情况来看，其中 69 家机构得分高于或等于平均值 853，36 家机构得分低于平均值，最低分数为 379 分。

1.2. 互联网资产统计

安全值对互联网资产进行分析统计，包括各机构注册的域名、面向互联网开放的主机服务（不仅限于 Web 服务的网站）和公网 IP 地址。

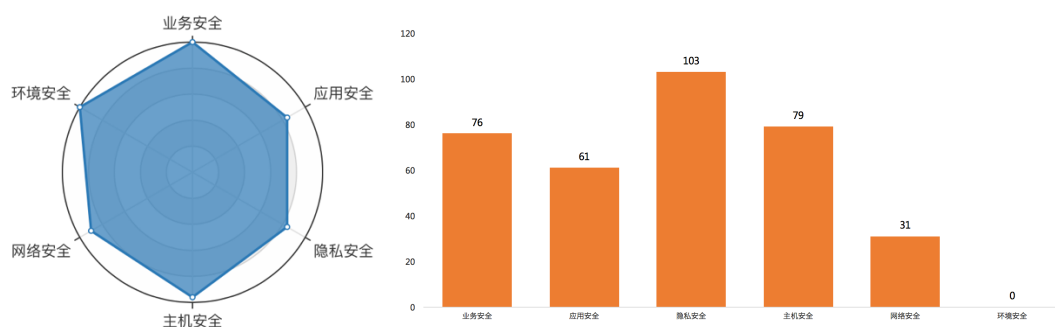


	域名数量	主机数量	IP 数量	平均每机构资产数量
总体	454	2510	2275	50

105 家保险公司的域名共有 454 个，公网主机 2510 个，公网 IP 地址 2275 个，平均每个公司有 50 个互联网资产。

2. 风险分布及量化评估

根据业内的信息安全风险管理最佳实践，结合风险等级、影响范围、频率、数量、时间各方面要素建立量化风险的计算模型，对整体情况的 6 个风险域（业务安全、应用安全、隐私安全、主机安全、网络安全和环境安全）进行量化评价。



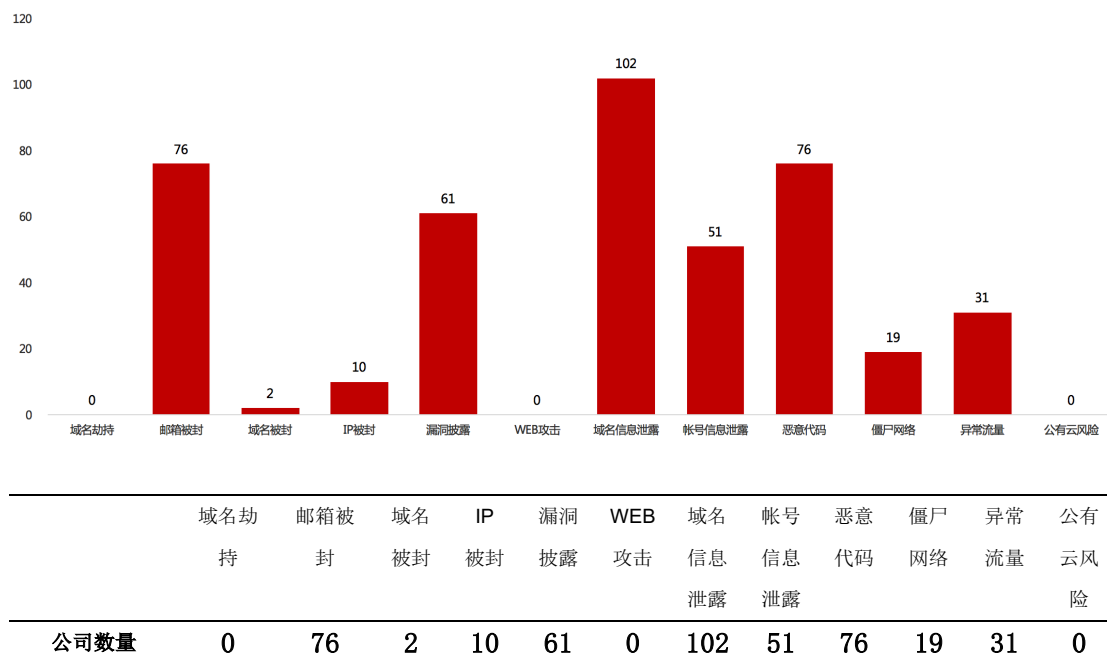
	机构数量	业务安全	应用安全	隐私安全	主机安全	网络安全	环境安全
公司数量	105	76	61	103	79	31	0

通过安全值对保险业第一季度的数据，进行量化风险发现：

应用安全、隐私安全和网络安全问题较为严重，三类风险中 61 家（58%）保险公司存在应用安全问题；103 家（98%）公司存在隐私安全问题；31 家（30%）存在网络安全问题，在线业务系统遭受到 DDOS 攻击，报告第 4 章将进行详细分析。

3. 风险指标分析

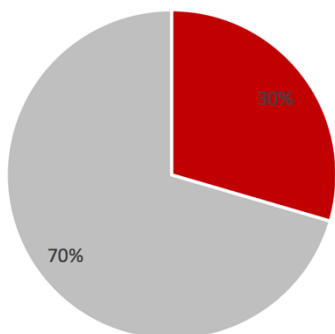
安全值整体基于 12 个风险指标支撑 6 个维度的安全评价，分别对各项风险指标影响的公司数量进行统计便于找出较集中的问题。



4. 异常流量风险详细分析

互联网上的应用系统或网络遭受到 DDOS 拒绝服务攻击，包括 TCP 攻击或 UDP 攻击的报警信息，拒绝服务攻击通过流量攻击的方式攻击系统或网络，持续遭受攻击或过大的攻击流量，可能引起系统服务中断。

异常流量



105 家保险公司中有 31 家机构（30%）遭受到 DDOS 攻击，构成了网络安全威胁的主要问题。

近 90 天内共发现 1346 次 DDOS 攻击记录，影响到 32 个 IP 地址。

根据对 90 天内 1346 次攻击的统计分析，攻击源地址共 69 个，通过在全球黑名单中进行查询，发现 17 个是黑名单地址，为较高威胁的攻击源地址，建议行业用户进行监控。

较高威胁的攻击源地址列表

攻击源	数量	黑名单	IP 信息
001.202.225.154	331	yes	北京市北京市 电信
061.139.073.071	11	yes	四川省成都市 电信
042.081.064.062	8	yes	天津市天津市 电信
106.226.059.093	7	yes	江西省宜春市 电信
106.226.058.248	7	yes	江西省宜春市 电信
036.022.032.178	7	yes	浙江省宁波市 电信
036.110.120.124	7	yes	北京市北京市 电信
036.042.035.193	7	yes	陕西省宝鸡市 电信
101.081.033.053	7	yes	上海市上海市 电信
001.080.041.242	7	yes	陕西省西安市 电信
218.005.076.086	6	yes	福建省厦门市 电信
036.022.037.210	4	yes	浙江省宁波市 电信
162.246.016.019	3	yes	美国
202.108.196.162	1	yes	北京市北京市 联通
219.234.088.035	1	yes	北京市丰台区 北京华夏联动网络有限公司 鹏博士宽带
106.039.097.131	1	yes	北京市北京市 电信
090.043.176.198	1	yes	法国

以下为遭受到攻击 IP 地址 Top10，116.213.76.41 受到的攻击次数最多，共计 525 次。

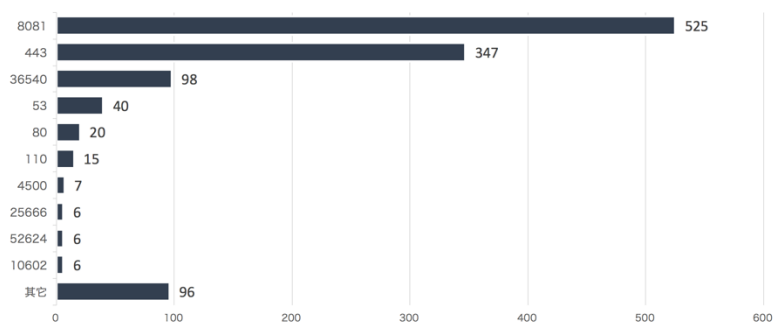
被攻击 IP 地址 Top 10

被攻击 IP	攻击数量
116.213.76.41	525

123.127.246.47	331
218.17.200.230	99
111.20.168.69	98
116.31.80.184	72
116.31.80.142	63
223.5.5.5	21
58.251.18.196	20
116.228.146.34	15
1.202.223.190	14

以下为遭受到攻击端口 Top10，端口 8081、443 分别遭受 525 次和 347 次攻击。

被攻击端口 Top 10



被攻击端口	攻击数量
8081	525
443	347
36540	98
53	40
80	20
110	15
4500	7
10602	6
52624	6
25666	6
其它	81

处置建议:

1. 监控在线系统的网络流量，尤其在“被攻击 IP 地址 Top 10”中的 IP 网络，根据异常流量影响出口带宽的情况选择运营商流量清洗或本地抗拒绝服务防护设备；
2. 参考“被攻击端口 Top 10”监控行业内风险较高的网络端口；
3. 建议监控“较高威胁的攻击源地址列表”中的地址，并采取控制措施；
4. 制定完善安全事件应急响应流程，面对拒绝服务攻击能够及时应对。

附表：保险公司名单（字母排序，不分先后）

1	爱和谊日生同和财产保险（中国）
2	安邦财产保险
3	安邦人寿保险
4	安诚财产保险
5	安华农业保险
6	安联财产保险（中国）
7	安信农业保险
8	百年人寿
9	北大方正人寿
10	渤海财产保险
11	诚泰财产保险
12	大众保险
13	鼎和财产保险
14	东京海上日动火灾保险（中国）
15	东吴人寿
16	都邦财产保险
17	丰泰保险（亚洲）有限公司上海分公司
18	复星保德信人寿
19	富邦财产保险
20	富德生命人寿保险
21	光大永明人寿保险
22	国华人寿保险
23	国泰财产保险
24	国泰人寿保险
25	国元农业保险
26	海康人寿保险
27	合众人寿保险
28	和谐健康保险
29	恒安标准人寿保险
30	弘康人寿
31	华安保险
32	华汇人寿
33	华农财产保险
34	华泰保险
35	华夏人寿
36	华信财产保险
37	汇丰人寿保险
38	锦泰财产保险
39	君龙人寿

40	昆仑健康保险
41	劳合社保险（中国）
42	乐爱金财产保险（中国）
43	利安人寿
44	利宝保险
45	美亚财产保险
46	民安财产保险
47	民生人寿
48	前海人寿
49	丘博保险（中国）
50	日本财产保险（中国）
51	日本兴亚财产保险（中国）
52	瑞泰人寿保险
53	三井住友海上火灾保险
54	三星财产保险
55	苏黎世保险公司北京分公司
56	太阳联合保险（中国）
57	泰康人寿
58	泰山财产保险
59	天安人寿保险
60	天平汽车保险
61	现代财产保险（中国）
62	新光海航人寿
63	新华保险
64	鑫安汽车保险
65	信诚人寿
66	信利保险（中国）
67	信泰人寿保险
68	阳光保险
69	阳光农险
70	英大泰和财产保险
71	英大泰和人寿
72	永安财产保险
73	永诚保险
74	友邦保险
75	长安责任保险
76	长城保险
77	长江财产保险
78	长江养老
79	长生人寿保险
80	招商信诺人寿保险
81	浙商财产保险
82	正德人寿保险

83	中德安联人寿保险
84	中法人寿
85	中国平安
86	中国人保集团
87	中国人寿集团
88	中国太保
89	中国太平
90	中航安盟保险
91	中航三星人寿保险
92	中荷人寿保险
93	中宏人寿保险
94	中煤财产保险
95	中美联泰大都会人寿
96	中融人寿
97	中新大东方人寿保险
98	中意财产保险
99	中意人寿
100	中英人寿保险
101	中邮人寿保险
102	中再集团
103	众诚汽车保险
104	珠江人寿
105	紫金财产保险