2018 年主流品牌与零售商（Top50）网络安全报告

（2018 年 1 月-5 月）

安全值

二零一八年五月

目录

第1章 概述

近年来，在大数据、云服务、人工智能等技术的推动下，零售业正在发生新变化。越来越多的零售企业把业务扩展到互联网上，不仅让消费者购物更加便捷，也极大扩展了销售渠道。但问题亦随之而来，如何有效保护消费者信息和关键数据？如何确保信息系统可有效抵御外部攻击？更多的网络安全问题正在成为零售企业发展互联网业务的挑战。

“安全值”利用大数据技术，对 58 家零售企业的网络风险状况进行了分析。根据零售企业的业务模式、产品类型，我们将采样的 58 家企业分为三类：零售商、快消品企业和电子产品企业，对这 3 类企业的互联网资产、安全风险进行了识别和分析。（企业名单详见第八章）

报告识别、分析的零售企业互联网资产主要包括注册的域名、线上的主机、IP 网络以及公有云迁移的情况。云技术的应用在方便业务、优化 IT 资源的同时，也使网络威胁发生变化，云化的信息系统为零售企业引来了新型风险。

报告对安全漏洞、网络攻击、垃圾邮件、隐私保护、恶意代码、僵尸网络和黑名单这 7 种典型互联网威胁进行分析，对采样的 58 家零售企业进行综合评分，评估其面临的安全风险。评分是基于客观、明确的外部安全数据，建立 R（互联网风险）、S（互联网资产规模）、T（风险趋势）、P（访问流行度）这 4 个维度评价指标，经过科学算法计算而形成，主要用于相同测量标准下的安全状况和趋势差异对比。

第2章 零售企业分类评价

2.1 零售企业安全值四维评价

企业分类	风险指数（R）	资产规模（S）	风险趋势（T）	流行度（P）
电子产品企业	319	7.5	-24	38.1
快消品企业	499	4.3	-14	22.3
零售商	576	5.3	-12	36.8
总计	475	5.3	-16	29.9

对各类零售企业进一步研究发现：电子产品企业的平均访问流行度、平均资产规模和平均风险指数最高；快消品企业由于不依靠自身进行线上销售，故访问流行度较低，但安全风险较高；全部采样企业的平均风险指数小于 600 分，整体处于高风险等级。

名词解释：

- **风险指数（R）：Risk，评分区间（0-1000 分），风险越高 R 值越低。**
- **风险评级：R 值＜599 分，高风险；600 分＜R 值＜899 分，中等风险；R 值＞900 分，低风险。**
- **资产规模（S）：Scale，评分区间（0-10 分），企业的资产数量越多 S 值越高。**
- **风险趋势（T）：Trend，评分区间（±1000 分），当月与前一月 R 值变化趋势。**
- **流行度（P）：Popular，评分区间（0-100 分），被访问次数越多 P 值越高。**

2.2 零售企业网络资产概况

58 家零售企业发现互联网资产共计 85494 个，包括注册的域名 367 个，面向互联网可访问的主机地址 71217 个，以及公网开放的 IP 地址 13910 个，为分析各类企业的线上业务开展状况，对企业的网络资产进行评估。结果如下表所示：

企业分类	风险指数	平均域名数	平均主机数	平均IP 地址数	云迁移企业比例	云资产比例
电子产品企业	319	6	2960	640	29%	5%
快消品企业	499	6	99	56	17%	18%
零售商	576	7	1795	222	27%	16%
总计	475	6	1228	240	22%	10%

安全值对这 3 类零售企业分析，发现以下特点：

① 电子产品企业、零售商的网络风险与资产规模成正比，资产规模越大，面临的网络风险越高；

② 电子产品企业和零售商的互联网资产规模庞大，平均资产量远高于快消品企业，这两类企业对于线上商业行为的依赖程度更高；

③ 快消品企业的资产数量少，但面临的安全风险仍然较高；

④ 少量企业应用云服务，应用云服务的企业数量占总比例的 22%，云资产数量占总资产量的 10%。

域名：组织经过 ICP 备案的域名；

主机：面向互联网开放的主机服务地址（例如 Web 网站、Email 服务、接口服务、业务系统等）；

IP 地址：在线系统使用的 IP 地址（包括本地服务器、IDC 托管、云主机等）；

云迁移：有互联网资产属于云服务的企业。

第3章 风险详述

零售企业网络风险概况（发生风险的企业数量占比）：

企业分类	风险指数	安全漏洞	网络攻击	隐私保护	垃圾邮件	恶意代码	僵尸网络	黑名单
电子产品企业	319	100%	64%	100%	0%	57%	14%	14%
快消品企业	499	62%	38%	97%	0%	17%	10%	21%
零售商	576	53%	47%	87%	0%	20%	7%	0%
总计	475	69%	47%	95%	0%	28%	10%	14%

根据上表发现，电子产品企业面临的互联网风险最高，100%的电子产品企业近一年内出现安全漏洞；庞大的业务量导致 64%的电子产品企业和 47%的零售商成为 DDOS 攻击的目标；恶意代码、僵尸网络风险在 3 类企业中都有发生，一旦企业发生恶意代码或僵尸网络事件，都可能导致业务中断事件的出现；值的注意的是，目前零售业整体已有 10%的企业存在 IP 地址被列入国际黑名单中，收录国际黑名单的安全设备将会阻断黑名单中 IP 地址的通讯，对线上业务的开展造成很大影响；此外研究发现 95%的零售企业存在域名注册人信息泄露的现象，建议及时对域名注册隐私信息实施保护，防止钓鱼邮件等社会工程学攻击利用企业暴露在外的信息。

第4章 安全漏洞分析

4.1 零售企业安全漏洞形势不容乐观

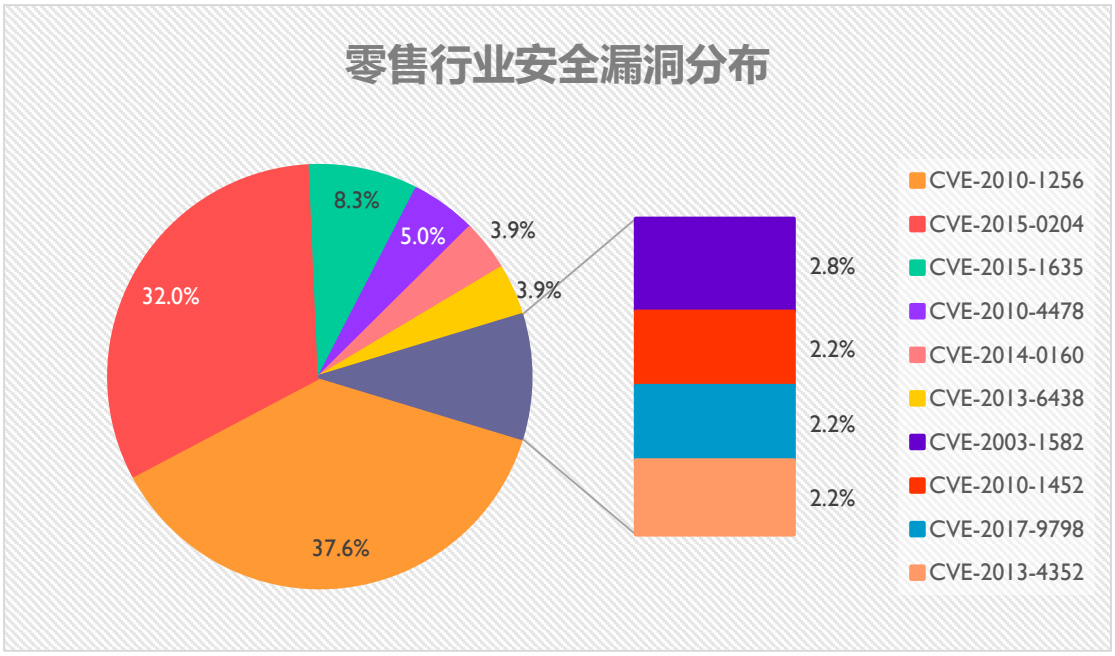
零售企业安全漏洞表：

企业分类	参与识别的企业数	出现漏洞的企业占比	漏洞数量
电子产品企业	14	100%	261
快消品企业	29	62%	131
零售商	15	53%	64
总计	58	69%	456

根据上表，采样的 58 家企业 2018 年至今出现安全漏洞 456 个，出现安全漏洞的企业占总数的 69%，14 家电子产品企业出现安全漏洞达 261 个；其中 100%的电子产品企业都出现了安全漏洞，零售商 53%出现安全漏洞。

上述现象说明个别企业目前对于互联网应用系统的安全漏洞缺乏有效管理、修复机制，容易被攻击者利用，可能会业务安全和用户敏感信息造成威胁。

4.2 安全漏洞一览（前 10 位）



4.3 漏洞统计与描述

漏洞类型	漏洞统计	漏洞描述
IIS 身份验证内存损坏漏洞 CVE-2010-1256	68	Internet Information Services (IIS)远程执行代码漏洞。漏洞是由于不正确地分析身份验证信息造成的。成功利用此漏洞的攻击者可以在工作进程标识(WPI)的上下文中执行代码。
OpenSSL 加密问题漏洞 CVE-2015-0204	58	由于 OpenSSL 库里的 s3_clnt.c 文件中，ssl3_get_key_exchange 函数，允许客户端使用一个弱 RSA 秘钥，向 SSL 服务端发起 RSA-to-EXPORT_RSA 的降级攻击，以此进行暴力破解，得到服务端秘钥。此问题存在于 OpenSSL 版本 0.9.8zd 之前，或 1.0.0p 之前的 1.0.0，或 1.0.1k 之前的 1.0.1。
Windows HTTP.sys 远程执行代码漏洞 CVE-2015-1635	15	使用 Microsoft IIS 6.0 以上版本的 Microsoft Windows 的 HTTP 协议堆栈(HTTP.sys)中存在远程执行代码漏洞，该漏洞源于 HTTP.sys 文件没有正确分析经特殊设计的 HTTP 请求。成功利用此漏洞的攻击者可以在系统帐户的上下文中执行任意代码。
OpenSSH J-PAKE 授权问题漏洞 CVE-2010-4478	9	当启用 J-PAKE 时，OpenSSH 5.6 及更早版本无法正确验证 J-PAKE 协议中的公共参数，该协议允许远程攻击者绕过了解共享密钥的需求，并成功进行身份验证。
Heartbleed 心脏滴血漏洞 CVE-2014-0160	7	OpenSSL Heartbleed 模块存在一个 BUG，问题存在于 ssl/dl_both.c 文件中的心跳部分，当攻击者构造一个特殊的数据包，使 memcpy 函数把 SSLv3 记录之后的数据直接输出，该漏洞导致攻击者可以远程读取存在漏洞版本的 OpenSSL 服务器内存中多达 64K 的数据。
Apache HTTP Server 拒绝服务漏洞	7	2.4.8 之前的 Apache HTTP 服务器的 mod_dav 模块中的 main / util.c 中的 dav_xml_get_cdata 函数未正确删除

漏洞类型	漏洞统计	漏洞描述
CVE-2013-6438		CDATA 节中的空白字符，这允许远程攻击者通过制作的 DAV 导致拒绝服务（守护进程崩溃）写请求。
IIS6.0 远程执行代码漏洞 CVE-2003-1582	5	IIS6.0 版本漏洞，款客户端 IP 地址启用 DNS 解析时，允许远程攻击者通过 HTTP 请求结合编写的 DNS 响应将任意文本注入日志文件中。如注入 XSS 序列所示，与“反向查找日志损坏（ILC）”问题有关。
Apache HTTP Server 进程崩溃漏洞 CVE-2010-1452	4	2.2.16 之前的 Apache HTTP Server 2.2.x 中的（1）mod_cache 和（2）mod_dav 模块允许远程攻击者通过缺少路径的请求导致拒绝服务（进程崩溃）。
Http Options 出血漏洞 CVE-2017-9798	4	Options 出血是在 Apache http 中释放错误后使用的，这会导致在响应 HTTP 选项请求时构造一个损坏的 Allow 标头。会泄漏可能包含机密的服务器进程中的任意内存片断。在多个请求之后,内存块会发生变化,因此对于易受攻击的主机,可泄漏任意数量的内存块。
Apache HTTP Server 拒绝服务漏洞 CVE-2013-4352	4	Apache HTTP Server 2.4.6 中的 mod_cache 模块的 modules / cache / cache_storage.c 中的 cache_invalidate 函数在启用缓存转发代理时允许远程 HTTP 服务器导致拒绝服务（NULL 指针解引用和守护进程崩溃） 通过触发缺失主机名值的向量。

第5章 网络攻击威胁快消品企业

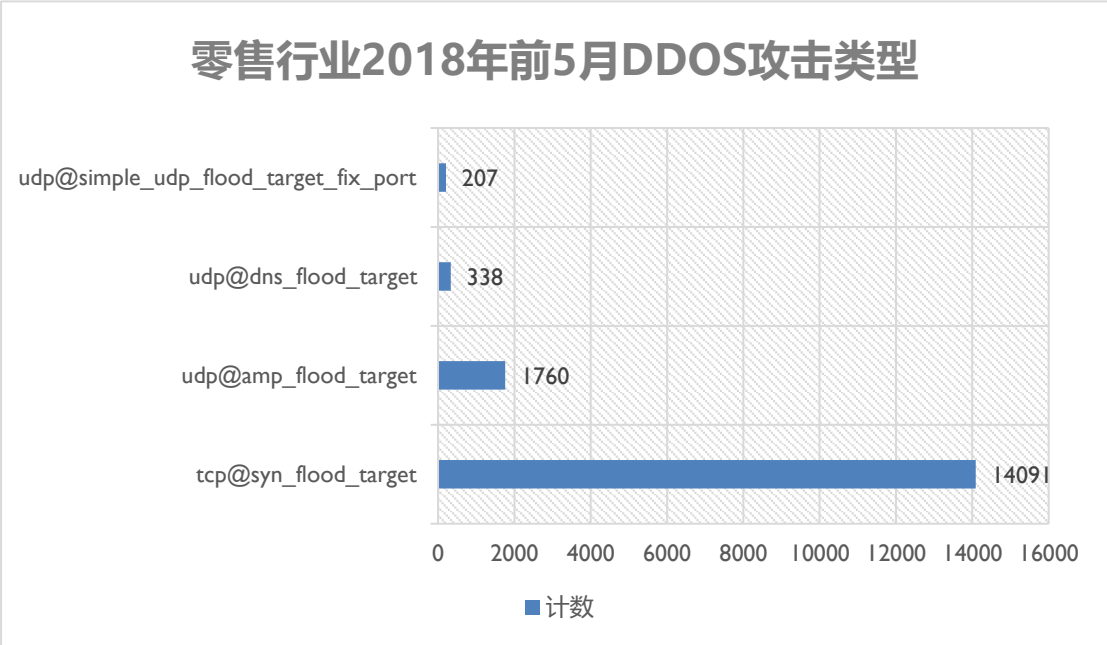
5.1 零售企业遭受网络攻击情况

企业分类	发生网络攻击的企业数量比	每家企业遭受网络攻击平均次数	每次网络攻击平均流量	遭受网络攻击的资产占总资产的比
电子产品企业	64%	1502	3108	5%
快消品企业	38%	313	11827	13%
零售商	47%	69	1878	6%
总计	47%	646	4796	7%

对零售企业遭受 DDOS 攻击的详细情况分析发现：电子产品企业遭受 DDOS 攻击的数量占比更大，达到 64%，平均每家遭受的攻击达 1502 次。38%的快消品企业遭受过 DDOS 攻击，由于快消品企业的互联网资产规模较小，遭受 DDOS 威胁的资产占总资产量达 13%，单次攻击的流量也最大，流量包数达 11827 个，远大于电子产品企业和零售商。可知 DDOS 攻击对于快消品企业造成的威胁较大。

大流量、高密度的 DDOS 攻击会对该领域企业的线上服务造成极大不良影响，这类企业应当使用流量清洗类服务以应对异常的大流量攻击，而遭受攻击频繁的企业在使用上述方法的同时，应对发起攻击次数高的可疑 IP 地址实施控制。

5.2 DDOS 攻击类型主要有 2 种



2018 年 1-5 月零售行业遭受 DDOS 攻击总计 16594 次，详细见下表：

攻击类型	攻击次数	占比
tcp@syn_flood_target	14091	84.9%
udp@amp_flood_target	1760	10.6%
udp@dns_flood_target	338	2.0%
udp@simple_udp_flood_target_fix_port	207	1.2%
tcp@ack_flood_target	198	1.2%

根据上表结果，TCP 半连接攻击占据网络攻击的主要部分，对于这种类型的 DDOS 攻击，可通过缩短 SYN 响应时间或设置 SYN Cookie 过滤 TCP 包等手段来实施。对于 UDP 放大攻击，可以通过限制 UDP 包大小，或建立 UDP 连接规则来达到过滤恶意 UDP 包，减少攻击发生的效果。可根据企业自身的详细情况选择合适的解决方案。

第6章 避免互联网资产出现于黑名单中

根据第 4 章风险概况表，可知有 14%的零售企业存在 IP 黑名单风险，主要集中在电子产品企业和快消品企业中。黑名单信息见下表：

IP 黑名单信息	IP 地址进入黑名单次数
alienvault	37
zeustracker.abuze	16
bambenekconsulting	10
teamcymru	3
the-haley	1

由于 IP 黑名单会被某些安全厂商的安全设备采用作为参考，故企业资产进入 IP 黑名单可能导致属于该企业的整个 IP 段被阻断通信，需要尽快向黑名单组织申诉解决。建议出现黑名单风险的企业根据向黑名单组织申诉的反馈结果来查询 IP 资产被列入黑名单的原因。

第7章 更多信息

本报告由“安全值”团队提供，如需更多、更详细数据请与我们取得联系。安全值是国内首个安全评价服务（SRS，SecurityRatingService）。目前正面向企业提供免费评估服务，您可访问安全值免费评估网站来获取您的企业评估报告。我们同样面向全国各行业的安全状况进行分析。如果您需要长期订阅安全值分析报告，可扫下方二维码进入“牛市”来订阅安全值年服务（全年每月一份安全值评估报告）。

联系我们：

- 安全值网站地址：https://www.aqzhi.com
- 安全值知识库：http://wiki.aqzhi.com
- 服务邮箱：support@aqzhi.com
- 联系电话：400-070-6887
- QQ：2674163033

安全值

2018 年 5 月

第8章 采样企业名单及分类（58 家随机排序）

序号	企业名称	分类	序号	企业名称	分类
1	苏宁云商	大型零售商	30	欧莱雅	快消品企业
2	京东	大型零售商	31	迪奥	快消品企业
3	华润万家	大型零售商	32	耐克	快消品企业
4	万达	大型零售商	33	伊利	快消品企业
5	麦德龙	大型零售商	34	中粮	快消品企业
6	淘宝	大型零售商	35	安利	快消品企业
7	欧尚	大型零售商	36	卡夫亨氏	快消品企业
8	永旺	大型零售商	37	百威英博	快消品企业
9	屈臣氏	大型零售商	38	蒙牛	快消品企业
10	亚马逊	大型零售商	39	宝洁	快消品企业
11	乐购	大型零售商	40	雀巢	快消品企业
12	沃尔玛	大型零售商	41	H&M	快消品企业
13	家乐福	大型零售商	42	可口可乐	快消品企业
14	百盛	大型零售商	43	红牛	快消品企业
15	天猫	大型零售商	44	玛氏箭牌	快消品企业
16	美的	电子产品企业	45	麦当劳	快消品企业
17	微软	电子产品企业	46	联合利华	快消品企业
18	苹果	电子产品企业	47	喜力	快消品企业
19	联想	电子产品企业	48	利洁时	快消品企业
20	华为	电子产品企业	49	加多宝	快消品企业
21	索尼	电子产品企业	50	三得利	快消品企业

22	飞利浦	电子产品企业	51	百事	快消品企业
23	LG	电子产品企业	52	亿滋国际	快消品企业
24	西门子	电子产品企业	53	强生	快消品企业
25	戴尔	电子产品企业	54	达能	快消品企业
26	惠普	电子产品企业	55	泰森	快消品企业
27	松下	电子产品企业	56	味好美	快消品企业
28	博世	电子产品企业	57	金佰利	快消品企业
29	日立	电子产品企业	58	道达尔	快消品企业