新零售生态网络安全报告

安全值

2018 年 6 月

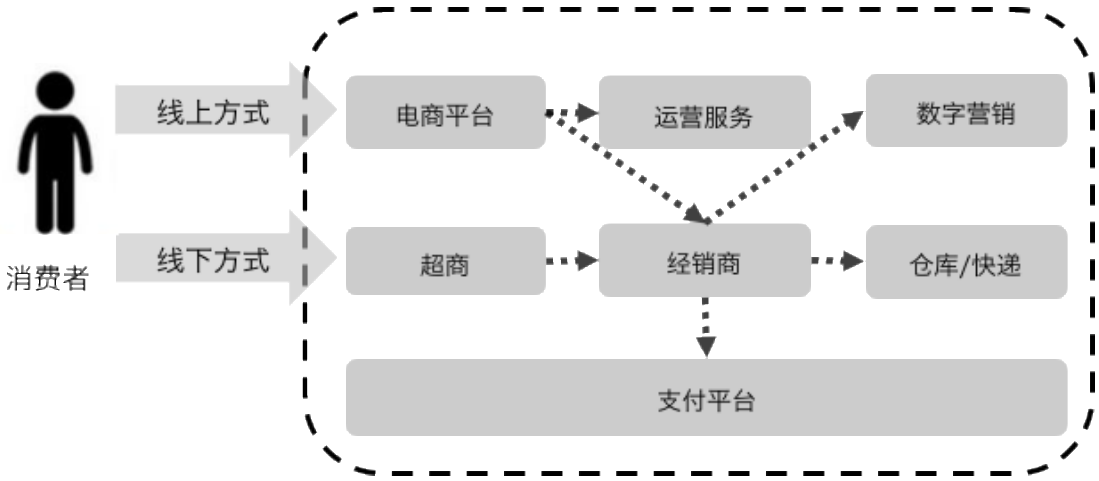
目录

第1章 报告介绍

1.1 概述

近年来，零售业蓬勃发展，规模持续扩大，业态不断创新，网络零售快速发展，在技术升级与消费升级驱动下，新零售应运而生；新零售强调通过大数据和互联网重构“人、货、场”等商业要素形成新的商业业态。

我国拥有 13 亿的消费人口，如何推动零售业持续、稳定、健康的发展是社会各界共同关心的课题。在以信息技术为驱动力，满足消费者多样性购物体验、“线上+线下”相结合的的新零售模式下，业务信息、个人信息、支付信息等都全面实现了采集网络化、信息共享化、支付通用化。在国家网络安全工作的深入推广、个人信息保护的高压态势下，敏感数据、个人隐私保护成为全社会关注的重点，报告通过对“新零售”生态链上下游企业和“消费者信息”的关系，选择了 8 个重要的环节，对在国内从事各环节业务的主流企业进行采样，包括：



1) 电商平台 30 家：用户线上消费的入口，国内主流电商平台；
2) 大型商超 20 家：线下综合类大型卖场、超市（部分也开展互联网转型）；
3) 消费品牌 40 家：消费者购买的国内外品牌生产厂商；
4) 数字广告 30 家：提供营销数据分析和程序化广告投放的服务企业；
5) 运营服务 30 家：为品牌主提供线上店铺运营和客户服务外包的服务企业；

6) 三方支付 30 家：拥有支付牌照的第三方支付公司；

7) 物流仓储 35 家：主流的仓储及配送服务企业；

8) 信息技术 30 家：提供公有云服务的云计算服务提供商。

为了解“消费者隐私”在新零售生态内的安全状况，报告对以上 8 类共计 245 家“新零售”上下游企业在 2018 年 618 期间的互联网资产、安全事件和脆弱性这三类数据进行计算分析，洞察产业链生态中的薄弱环节与主要网络风险。

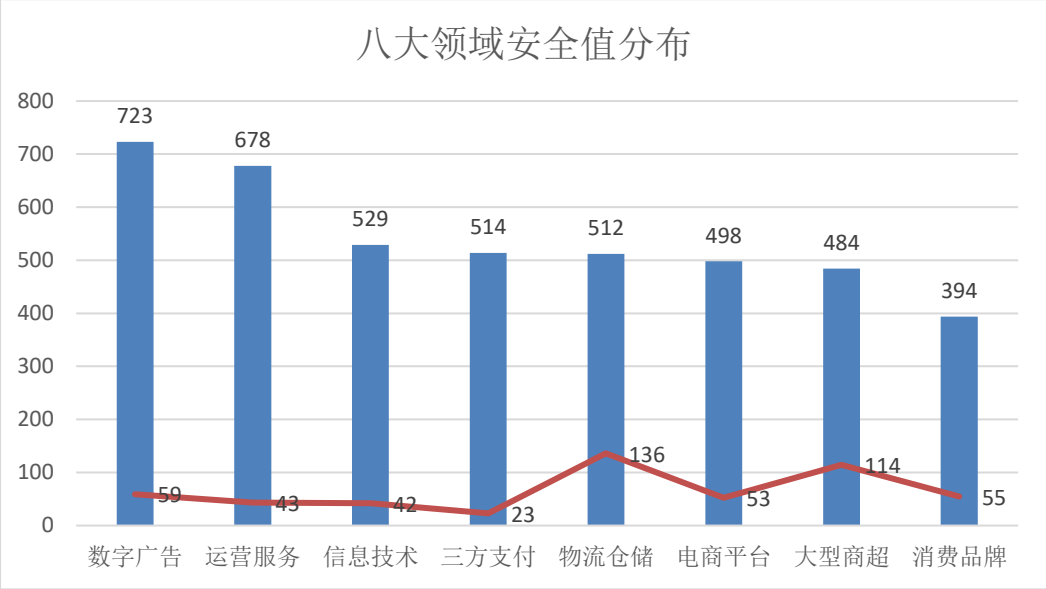
618 大促始于 2009 年，源于京东店庆月。随着促销的常态化，618 逐渐演变成全民购物节。每年的 618 大促对于新零售企业来说，都是一次大考。我们作为中立性网络安全与风险服务机构，认为此期间的数据更具代表性，更可体现相关企业的网络安全状况，因此，我们将本报告数据采集时间定为 2018 年 4 月 1 日-2018 年 6 月 20 日。

1.2 名词解释

- **安全漏洞：**主机操作系统和安装的组件存在的严重的高危漏洞，会使服务器遭受病毒或黑客入侵，引起信息泄露或篡改。
- **网络攻击：**企业在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，过大的攻击流量会引起服务中断。
- **垃圾邮件：**组织邮箱服务器被列为垃圾邮件发送域，一旦被反垃圾邮件设备拦截，将导致用户可能无法正常使用邮件。
- **恶意代码：**来自国内外安全厂商的恶意代码检测结果，系统可能已经被植入后门、病毒或者恶意脚本。
- **僵尸网络：**组织服务器被攻破，被当做“肉鸡”不断向外部发起扫描或者攻击行为，服务器主机可能被入侵，存在后门被远程控制。
- **黑名单：**域名或者 IP 地址被权威黑名单机构列入黑名单，用户的正常网页访问可能被浏览器拦截或者 IP 网络通讯被防火墙阻断。

第2章 “新零售”八大领域安全矩阵

2.1 八大领域安全风险值概况



注：安全值越低则风险越高

通过数据分析可以发现在八大领域取样的企业中，数字广告类企业平均风险值最高为 723；消费品牌企业平均风险值最低为 394；在《网络安全法》、欧盟 GDPR 法案对个人隐私保护强烈态势下，一直崇尚精准营销的数字广告行业安全工作受到了挑战，虽然在“新零售”的八个领域中表现最佳，但 723 分在全国各行业中属于偏低水平，安全能力提升空间还很大。而消费品牌企业则更加侧重于产品生产、营销，对安全工作的投入较少，394 分体现了这一点。图中红色曲线代表了八类企业近一个月安全状况的趋势图，其中可以看到物流仓储及大型商超类在近一个月来安全值增长最快，其他行业也均为增长趋势。

2.2 八大领域安全值四维评价

行业领域	风险值（R）	资产规模（S）	风险趋势（T）	访问流行度（P）
物流仓储	512	4.0	136	23.9
大型商超	483	4.3	114	28.7
三方支付	516	4.7	23	29.9
电商平台	497	6.3	53	41.9
运营服务	683	3.1	43	20.0
信息技术	562	5.1	42	26.6

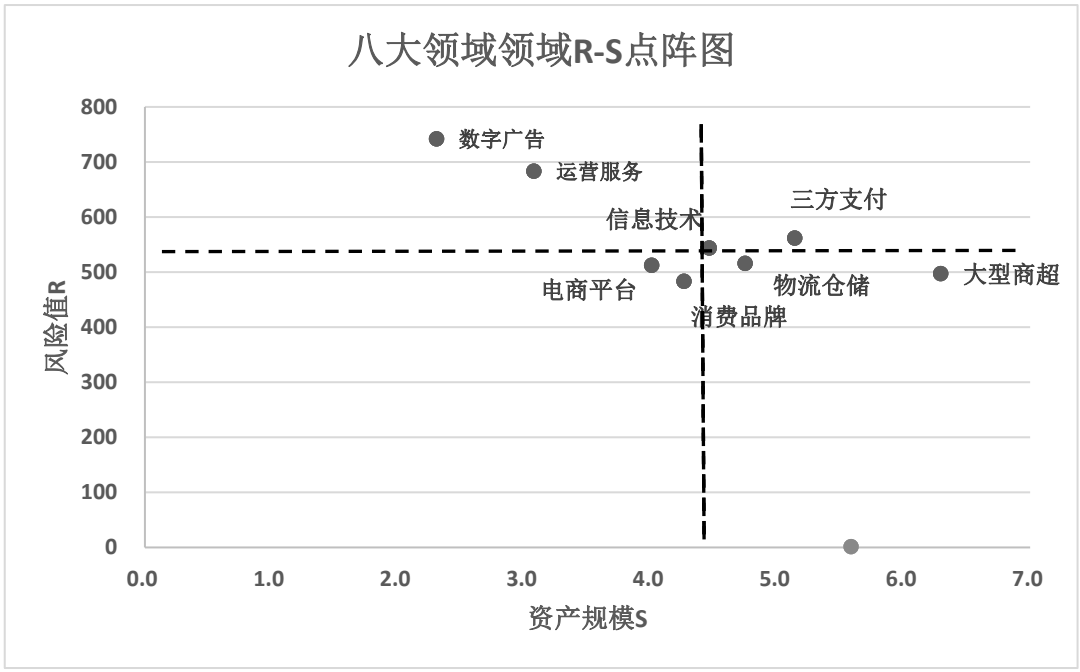
数字广告	742	2.3	59	18.4
消费品牌	394	5.6	55	29.4

为了能够深入研究行业互联网风险状况及关联，我们采用 RSTP 四维评价模式，从风险值、资产规模、风险趋势、流行度等角度的数据分析了各领域风险状况及其内在关系。从上表可以看出八大领域中电商平台的互联网资产规模最大，物流仓储风险值较上月增幅较大，同样访问流行度最高的行业为电商平台，也意味着电商平台采集的个人信息最多。

名词解释：

- **风险值（R）：Risk，评分区间（0-1000 分），风险越高 R 值越低。**
- **资产规模（S）：Scale，评分区间（0-10 分），机构的资产数量越多 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。**

2.3 八大领域资产 S-R 风险相关关系分析



为了研究资产数量对网络风险的影响，我们根据表中的数据绘制了象限图，从图中可以看出，抽样企业的风险值随着资产数量增多而降低，图中虚线代表了

平均资产数量及平均风险值；我们认为位于第一象限的三方支付是风险值最高的领域，在单位资产中风险均分较高；而作为资产数量最多的电商平台及消费品牌则风险值最低，说明互联网资产的增多一定程度上增加了互联网暴露面，为企业带来了更多的互联网风险，企业必须采取更加科学的体系完善安全工作。

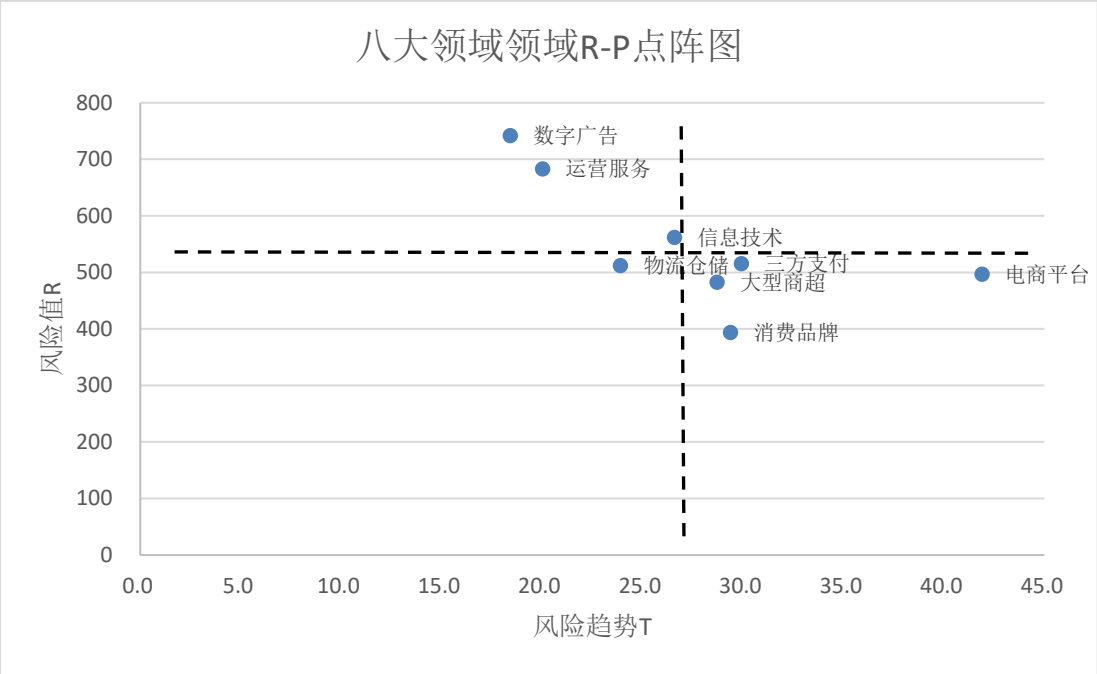
我们为了分析八大领域资产的详细情况，将互联网资产分为域名资产、主机资产、IP 资产、云资产等几个维度进行统计结果如下：

行业领域	风险值	域名平均数	主机平均数	IP 地址平均数	云迁移企业比例	云资产比例
物流仓储	511	3	5414	91	55%	7%
大型商超	483	4	262	60	40%	2%
三方支付	514	5	1058	107	50%	12%
电商平台	498	7	3678	224	73%	9%
运营服务	678	2	90	9	83%	41%
信息技术	528	3	1576	625	27%	23%
数字广告	723	1	16	7	33%	11%
消费品牌	394	6	2658	363	53%	2%

注：信息技术主要指“云计算”提供商，本次分析并未涵盖用户资源池 IP 地址。

从表中可以看出，域名数最多的为电商平台，平均每家电商有 7 个线上域名；主机数最多的是物流仓储领域；IP 资产最多的则是为企业提供云服务的信息技术类企业；其中提供运营服务的企业云资产比例、迁移比例均为最高，运营服务为很多商家提供售前、售后的外包服务，工作性质基于网络开展较多，接触的业务数据较为敏感，需要重点考虑其风险状况。

2.4 八大领域流行度 P-R 风险相关关系分析



为了研究访问流行度和网络风险的关系，我们根据表中的数据绘制了象限图，从图中可以看出，电商平台访问流行度最高；图中虚线代表了平均访问量及平均风险值，从风险趋势来看，访问流行度较高的三方支付、大型商超、消费品牌及电商平台的风险值均较低；访问流行度代表着企业互联网业务系统的访问频率及用户规模，越是活跃的业务系统重要性越高，但目前的安全风险却最高。

第3章 “新零售”八大领域网络风险分析

3.1 “新零售”八大领域网络风险概况

行业领域	风险值	样本数量	安全漏洞	网络攻击	隐私保护	恶意代码	僵尸网络	IP 黑名单
物流仓储	511	40	75%	40%	88%	20%	5%	3%
大型商超	483	20	75%	45%	100%	15%	10%	5%
三方支付	514	30	77%	43%	87%	7%	7%	17%
电商平台	498	30	40%	77%	80%	27%	13%	10%
运营服务	678	30	57%	7%	73%	7%	3%	0%
信息技术	528	30	70%	33%	83%	17%	17%	17%
数字广告	723	30	50%	7%	67%	0%	0%	3%
消费品牌	394	40	88%	63%	98%	38%	8%	20%
总计	536	250	67%	40%	84%	17%	8%	10%

我们从安全漏洞、网络攻击、隐私保护、恶意代码、僵尸网络、IP 黑名单等六个维度的网络风险数据对采样企业做了分析，根据上表发现，2018 年初至 618 结束，消费品牌企业面临的互联网风险最高；88%的消费品牌企业出现安全漏洞；庞大的线上业务量使电商平台遭受 DDOS 攻击占比达到 77%；大型商超的隐私保护问题高达 100%；恶意代码、僵尸网络风险相对发生率较低，数字广告的企业恶意代码及僵尸网络的发生率极低；其中消费品牌 38%的企业出现恶意代码，电商平台为 27%，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；目前提供云服务的信息技术类企业整体已有 17%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不良影响；同时消费品牌企业高达 20%的互联网业务平台被列入黑名单，特定浏览器将无法正常访问这些平台。

3.2 “新零售”八大领域安全漏洞详情

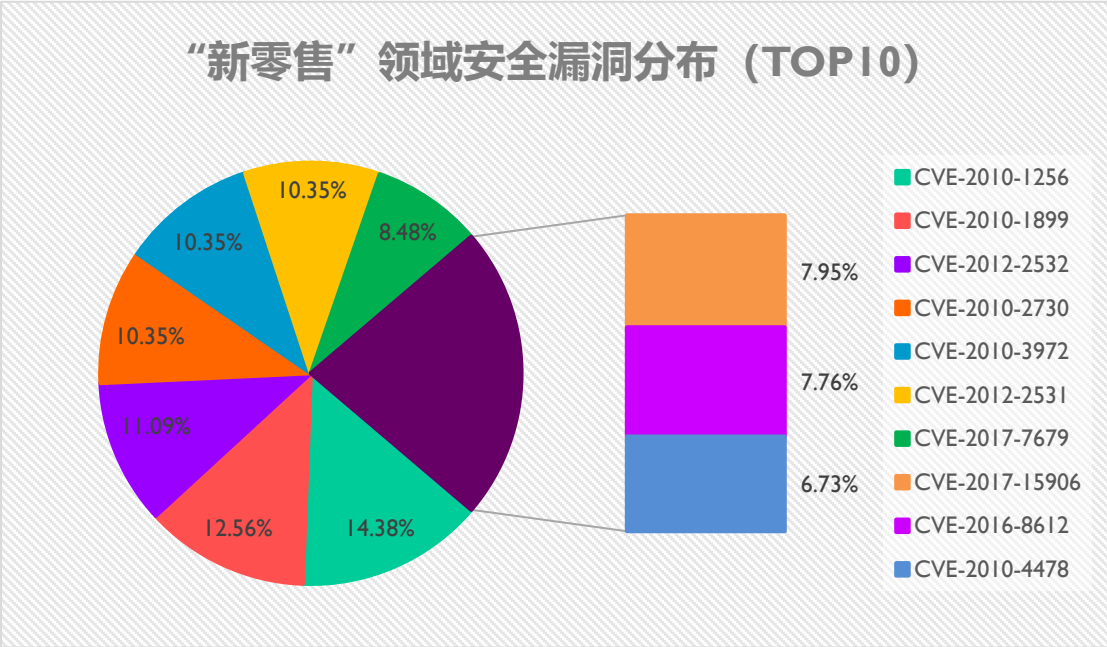
3.2.1 “新零售”八大领域安全漏洞概况

我们分析了八大领域安全漏洞的整体情况统计如下：

行业领域	风险值	样本数量	漏洞企业占比	平均漏洞数量
物流仓储	511	40	75%	75
大型商超	483	20	75%	68
三方支付	514	30	77%	29
电商平台	498	30	40%	93
运营服务	678	30	57%	25
信息技术	528	30	70%	90
数字广告	723	30	50%	25
消费品牌	394	40	88%	114

由上表可知，2018 年 4-6 月，“新零售”各类企业出现漏洞共计 16780 个，其中三方支付、消费品牌两类企业出现的安全漏洞占比最高；电商平台、消费品牌平均漏洞数量最多。所有企业发生漏洞的概率高于 67%，漏洞数量多于 65 个；高危漏洞一直都是危害业务系统正常运行、导致数据泄漏的元凶，就目前来看，“新零售”企业的漏洞问题非常严重，说明新零售企业整体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，可能会对新零售企业的业务安全和用户敏感信息造成威胁；作为供应链的整体信息流参与者，不光自己的漏洞，来自第三方的漏洞危害同样会危及到自身业务系统，建议新零售企业在做好内部漏洞管理的同时也要加强第三方企业漏洞风险管理。

3.2.2 采样企业中最常见安全漏洞一览



3.2.3 常见漏洞统计与描述

漏洞类型	数量统计	漏洞描述
Microsoft IIS 身份验证内存损坏漏洞 CVE-2010-1256	955	当启用了 Extended Protection for Authentication 时，Microsoft IIS 6.0、7.0 和 7.5 中未指定的漏洞允许远程认证用户通过与“标记检查”相关的未知向量执行任意代码，这些向量会触发内存损坏。
IIS 重复参数请求拒绝服务漏洞 CVE-2010-1899	834	Microsoft Internet 信息服务（IIS）5.1,6.0,7.0 和 7.5 中的 ASP 实现中的堆栈使用漏洞允许远程攻击者通过与 asp.dll 相关的精心制作的请求（守护程序中断）导致拒绝服务（又称“IIS 重复参数请求拒绝服务漏洞“。
IIS FTP 命令注入漏洞 CVE-2012-2532	736	用于 Internet 信息服务（IIS）的 Microsoft FTP 服务 7.0 和 7.5 在会话启用 TLS 前处理未指定的命令，这允许远程攻击者通过阅读对这些命令的回复来获取敏感信息。
IIS 请求标头缓冲区溢出漏洞 CVE-2010-2730	687	Microsoft Internet Information Services（IIS）7.5 中的缓冲区溢出在启用 FastCGI 时允许远程攻击者通过请求中的精心设计的标头执行任意代码。

漏洞类型	数量统计	漏洞描述
IIS FTP 服务堆缓冲区溢出漏洞 CVE-2010-3972	687	Microsoft FTP 服务 7.0 和 7.5 中 Internet 信息服务（IIS）7.0 和 IIS7.5 的 ftpsvc.dll 中 TELNET_STREAM_CONTEXT::OnSendData 函数内基于堆的缓冲区溢出漏洞允许远程攻击者执行任意代码或导致拒绝服务、守护进程崩溃）通过精心设计的 FTP 命令。
IIS 密码泄露漏洞 CVE-2012-2531	687	Microsoft Internet 信息服务（IIS）7.5 对操作日志使用较弱的权限，允许本地用户通过阅读该文件发现凭据。
Apache Httpd 读取字节漏洞 CVE-2017-7679	563	在 2.2.33 之前的 Apache httpd 2.2.x 和 2.4.26 之前的 2.4.x 之后，mod_mime 可以在发送恶意 Content-Type 响应头时读取缓冲区末尾的一个字节。
OpenSSH 写入错误漏洞 CVE-2017-15906	528	在 7.6 之前的 OpenSSH 中的 sftp-server.c 中的 process_open 函数不能正确地阻止只读模式下的写入操作，这允许攻击者创建零长度文件。
Apache HTTP Server httpd 进程分段漏洞 CVE-2016-8612	515	版本 httpd 2.4.23 之前的 Apache HTTP Server mod_cluster 容易受到负载平衡器中协议分析逻辑中的错误输入验证的影响，导致服务 httpd 进程中出现分段错误。
OpenSSH J-PAKE 授权问题漏洞 CVE-2010-4478	447	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，方法是发送精确的值 协议的每一轮都是与 CVE-2010-4252 相关的问题

CVE 漏洞比较容易被攻击者利用，会为攻击提供更便利的途径，对新零售企业的信息系统威胁较大，需要根据各种漏洞的特点实施修补。

3.3 “新零售”八大领域网络攻击详情

3.3.1 “新零售”八大领域网络攻击概况

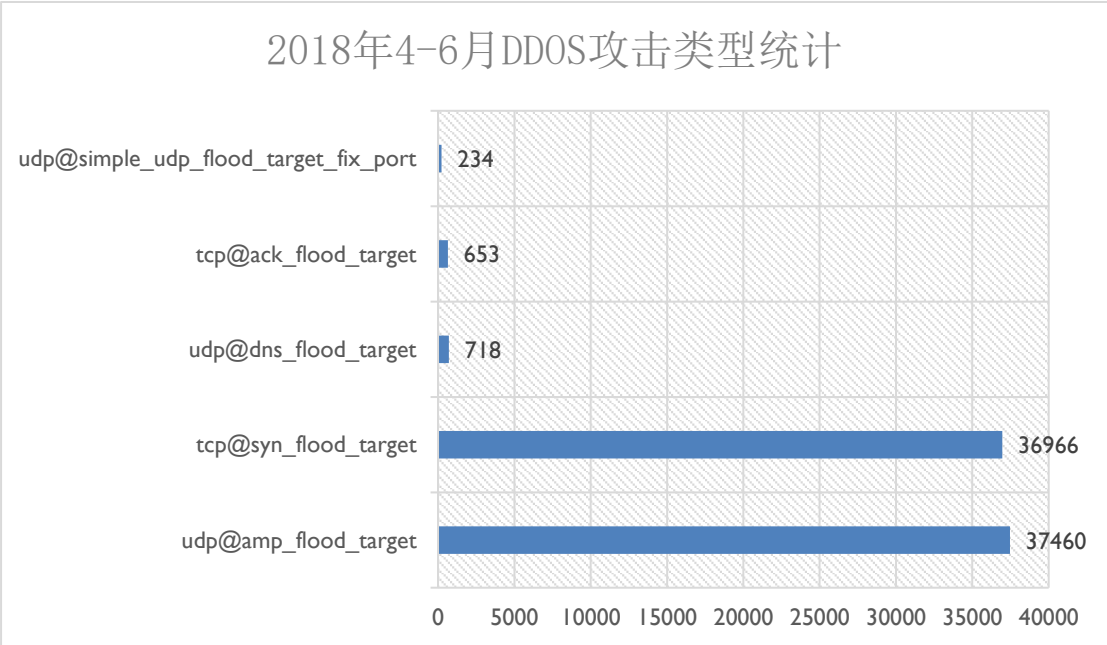
我们分析了“新零售”八大领域在 2018 年 4-6 月遭受 DDOS 攻击网络攻击情况统计如下：

行业领域	风险值	被网络攻击企业占比	平均每家企业遭受网络攻击次数	每次攻击平均流量	受影响资产占比
物流仓储	511	40%	151	1.1G	2%
大型商超	483	45%	8	1.8G	3%
三方支付	514	43%	820	2.1G	16%
电商平台	498	77%	87	7.6G	5%
运营服务	678	7%	36	0.4G	16%
信息技术	528	33%	184	12.0G	3%
数字广告	723	7%	30	21M	37%
消费品牌	394	63%	327	6.4G	4%
总计	536	40%	253	4.5G	5%

我们发现：电商平台、消费品牌企业遭受 DDOS 攻击的数量占比较大，企业占比高于 60%；三方支付类企业遭受 DDOS 次数最高，平均达到 820 次；信息技术类企业遭受 DDOS 攻击的平均流量高达 12G，远高于其他领域；大流量、高密度的 DDOS 攻击会对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。

3.3.2 采样企业常见攻击统计与描述

3.3.2.1 DDOS 攻击详情



详见下表：

DDOS 攻击类型	DDOS 攻击次数	占比
udp@amp_flood_target	37460	49.3%
tcp@syn_flood_target	36966	48.6%
udp@dns_flood_target	718	0.9%
tcp@ack_flood_target	653	0.9%
udp@simple_udp_flood_target_fix_port	234	0.3%

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。

3.3.2.2 恶意代码详情

我们同样研究了恶意代码对八类企业的影响：

行业领域	样本数量	风险值	恶意代码企业占比	平均每个主域名下恶意代码数量
物流仓储	40	511	8%	3
大型商超	20	483	3%	4
三方支付	30	514	2%	3
电商平台	30	498	8%	45
运营服务	30	678	2%	2
信息技术	30	528	5%	9
数字广告	30	723	0%	0
消费品牌	40	394	15%	6

从统计结果来看，消费品牌类的恶意代码比例高达 15%，而电商平台及物流仓储类企业的恶意代码比例也高达 8%，其中电商平台平均每个主域名下恶意代码数量居然达到 45 个，数字广告类的恶意代码数量则明显较少；恶意代码的产生原因多样，建议企业多关注外部威胁情报数据，尽早发现恶意代码链接，尽快处理恶意代码以免影响到页面的正常访问。

3.4 访问流行度 Top10 企业网络风险分析

我们排列了访问流行度最高的十家企业，分析了其中网络风险发生概率较大的企业如下：

公司名称	行业领域	R 值	S 值	P 值	总资产	网络攻击	信息泄露	恶意代码	安全漏洞
淘宝	电商平台	403	10.0	80.8	25669	182		556	
苹果	消费品牌	180	10.0	72.8	7006	193	1	20	29
大润发	大型商超	400	4.2	67.7	37	2	1		24
小米	消费品牌	169	10.0	65.6	47613	193	1	85	76
支付宝	三方支付	427	10.0	64.5	22351	9374			81
网易	电商平台	937	3.1	61.7	56		1		
京东	电商平台	146	10.0	60.9	13250	236	1	24	235
微软	消费品牌	176	10.0	58.3	27155	244	1	48	22
转转	电商平台	714	2.3	58.1	17		1		
优卖网	电商平台	716	3.8	55.0	2252		1		
阿里巴巴 1688	电商平台	734	10.0	53.5	12232	1			
天猫	电商平台	783	10.0	52.1	16188				
苏宁	大型商超	153	10.0	52.0	3691	36	1	7	147
质云	信息技术	317	8.2	52.0	2534	38	1		31
惠普	消费品牌	400	10.0	49.5	1326	2	1		332

我们可以看到这些企业不光访问流行度较高，资产数量相对也较高；淘宝的恶意代码数量高达 556 个，支付宝遭受的网络攻击高达 9374 次，惠普、京东的安全漏洞均高于 200 个，几乎所有的企业都有信息泄露的风险；这些都是国内外知名度较高的企业，资产数

量众多、用户范围庞大，一旦出现安全事件都会给企业和消费者带来巨大的损失。

3.5 资产数量 Top10 企业网络风险分析

我们选择了资产数量最多的十家企业分析了其网络风险的情况：

公司名称	领域	R 值	S 值	P 值	资产总数	网络攻击	僵尸网络	信息泄露	IP 被封	恶意代码	安全漏洞
中通	物流仓储	256	10	29	210585	153		1		2	2
小米	消费品牌	169	10	66	47613	193		1		85	76
微软	消费品牌	176	10	58	27155	244		1		48	22
淘宝	电商平台	403	10	81	25669	182				556	
联想	消费品牌	186	10	40	24012	3120		1		26	811
光环新网	信息技术	103	10	38	23382	264	327	1	7	4	894
支付宝	三方支付	427	10	65	22351	9374					81
阿里云	信息技术	174	10	47	18336	379				65	57
京东	电商平台	146	10	61	13250	236	2	1		24	235
阿里巴巴	电商平台	734	10	53	12232	1					
创锐文化	电商平台	241	10	41	11252	50		1		1	14
中彦信息	电商平台	136	10	41	8344	389	2	1	1		68
苹果	消费品牌	180	10	73	7006	193		1		20	29
易车信息	电商平台	152	10	43	3868	79		1	2	86	176
苏宁云商	大型商超	153	10	52	3691	36		1	3	7	147
优刻得	信息技术	314	10	38	3601		42	1			38

AZURE	信息技术	618	10	25	3384			1			16
金蝶软件（中国）有限公司	信息技术	120	10	43	3260	7		1	3	7	433
惠普贸易（上海）有限公司	消费品牌	400	10	49	1326	2		1			332

从表中可以看出中通作为资产最多的企业，网络风险主要来自于网络攻击，作为资产数量庞大的支付宝与联想也同样遭受着网络攻击的苦恼，光环新网、金蝶则网络漏洞数量庞大。

3.6 互联网威胁最大的十家企业网络风险分析

为了识别企业安全状况较差的核心原因，我们统计了互联网威胁最大的十家企业，将我们可以采集到的风险进行分析处理：

公司名称	行业领域	资产总数	DDOS次数	DDOS资产	僵尸网络流量	僵尸网络次数	僵尸网络资产	域名信息泄露	IP被封次数	恶意代码资产	恶意代码次数	安全漏洞
光环新网	信息技术	23382	264	36	46577	327	30	1	7	2	4	894
金蝶软件	信息技术	3260	7	1				1	3	2	7	433
海尔集团	消费品牌	1306	3	2	80	2	1	1	1	1	3	343
联动优势	三方支付	353	72	3				1	8	1	1	27
团博百众	电商平台	4183	57	8				1		2	5	128
中彦信息	电商平台	8344	389	2	8	2	1	1	1			68
华为	消费品牌	2476	974	28				1		4	77	83
腾讯云	信息技术	1417	195	17	4808	14	4	1	1			12
京东电商	电商平台	13250	236	68	33	2	2	1		1	24	235
美的集团	消费品牌	1063	389	8	8	2	1	1		1	1	458

易车信息	电商平台	3868	79	16				1	2	7	86	176

可以发现，网络攻击及安全漏洞是导致分值较低主要原因，但是恶意代码、信息泄露发生的概率较高也不可忽视；十家企业六个风险维度几乎都受到了影响。

第4章 报告总结

“新零售”与我们每个人的生活息息相关，电商交易系统不仅存有海量的用户敏感数据，而且直接涉及到资金交易。从分析数据可以看出零售行业面临着多种多样的安全威胁，安全漏洞、网络攻击、垃圾邮件、恶意代码、僵尸网络、黑名单等风险无时无刻不威胁着“新零售”生态链的各个环节企业，不光电商平台、三方支付平台需要加强信息安全管理，物流仓储、大型商超、运营服务、数字广告等企业也应该加强安全体系建设降低安全风险。从分析的结果来看，问题普遍较为严重的消费品牌一直是我们关注的盲区，其实作为产品的直接生产者，生态链的重要环节之一最需要建立完善的安全体系，不光要合规合法，更要时时关注安全动态、安全事件。

因此，“新零售”各个环节企业安全水平体现在能否快速响应网络攻击，做到快速识别风险、及时修补漏洞、提升员工安全意识以及积极引入威胁情报数据、完善网络安全防范机制等方面。

第5章 数据支持

本报告由“安全值”团队基于大数据分析结果提供，如需要更多、更详细的数据请与安全值取得联系。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，您可以访问安全值免费评估网站：https://www.aqzhi.com/来获取您企业自己的安全评估报告。安全值同样面向全国各行业的安全状况进行分析，获取行业报告请进入地址：https://www.aqzhi.com/themes/default/download.html。

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
- 数据咨询：18614003443
- QQ：2674163033

2018 年 6 月

第6章 企业名单

备注：以下排名不分先后，按企业名称首个字拼音排序。

电商平台	大型商超	消费品牌		三方支付	运营服务	数字广告	物流仓储		信息技术
1 号店	百安居	adidas	雀巢	Mo 宝支付	百秋网络	BBDO	DHL	振华	360 云
阿里巴巴	百盛	H&M	日立	百度钱包	宝尊	奥美	安得物流	中铁铁龙	AWS
贝贝	大润发	LG	三星	宝付支付	碧橙	北京广告	安能聚创	中通快递	AZURE
楚楚街	迪卡侬	LVMH 集团	松下	贝付	淳钲	博达大桥	百世物流	中外运	IBM 云
当当	国美	NIKE	微软	财付通	凡臣	达彼思	菜鸟网络	中远海运	speedycloud
返利网	红星美凯龙	SONY	西门子	国付宝	古星互联	电通	德邦物流		Ucloud
瓜子二手车	华联	百事	喜力	环迅支付	嗨购	分众传媒	飞马供应链		xyclouds
京东	华润万家	百威	小米	汇付天下	虎巴	葛瑞	国贸泰达		阿里云
京东到家	家乐福	宝洁	伊利	汇聚支付	君美瑞	广东省广告	华贸国际		百度云
聚划算	乐购	博世	亿滋国际	京东支付	蓝标电商	海润	嘉里大通		宝德云
聚美优品	联华	达能		快钱	乐其网络	恒美	建发		比格云
卷皮折扣	麦德龙	戴尔		拉卡拉	礼尚	凯络	锦程国际		华为企业云
礼物说	欧尚	飞利浦		连连支付	丽人丽妆	李奥贝纳	京东物流		华云数据
美丽说	苏宁	海尔		联动优势	联恩	灵思云途	联邦快递		金蝶云
蜜芽	万达	亨氏		平安壹钱包	流翔	灵智精实	全峰快递		金山云
蘑菇街	沃尔玛	红牛		钱宝	鹏泰博兴	龙韵传播	日日顺		浪潮云
拼多多	物美	华为		钱袋宝	青木数字	麦肯光明	上海交运		美团云
人人车	宜家	惠普		盛付通	瑞金麟	群邑	申通快递		鹏博士企业云

闪电降价	永辉	金佰利		双乾支付	上佰	睿狮	顺丰控股		七牛云
什么值得买	永旺	可口可乐		通联支付	速网	省广合众	天马迅达快递		青云
淘宝		利洁时		易宝支付	淘通	盛世长城	天天快递		世纪互联
天猫		联合利华		易极付	特思尔	思美传媒	象屿速传		曙光云
网易考拉		联想		易联支付	小冰火人	腾迈	新兴交通		腾讯云
网易严选		玛氏		易生支付	新七天	伟视捷	邮政速递		天翼云
唯品会		麦当劳		银联	兴长信达	玺桥传播	圆通速递		网宿云
闲鱼		美的		银盛支付	雅诺达	阳狮	远成物流		网易云
亚马逊		蒙牛		证联支付	艺零玖	智威汤逊-中乔	韵达控股		沃云
易车二手车		欧莱雅		支付宝	悠可	中航文化	宅急送快运		小鸟云
折 800		苹果		智付支付	悦为	中视金桥	长安民生		移动云
转转		强生		中金支付	卓益信息	众成就	长久物流		中企通信