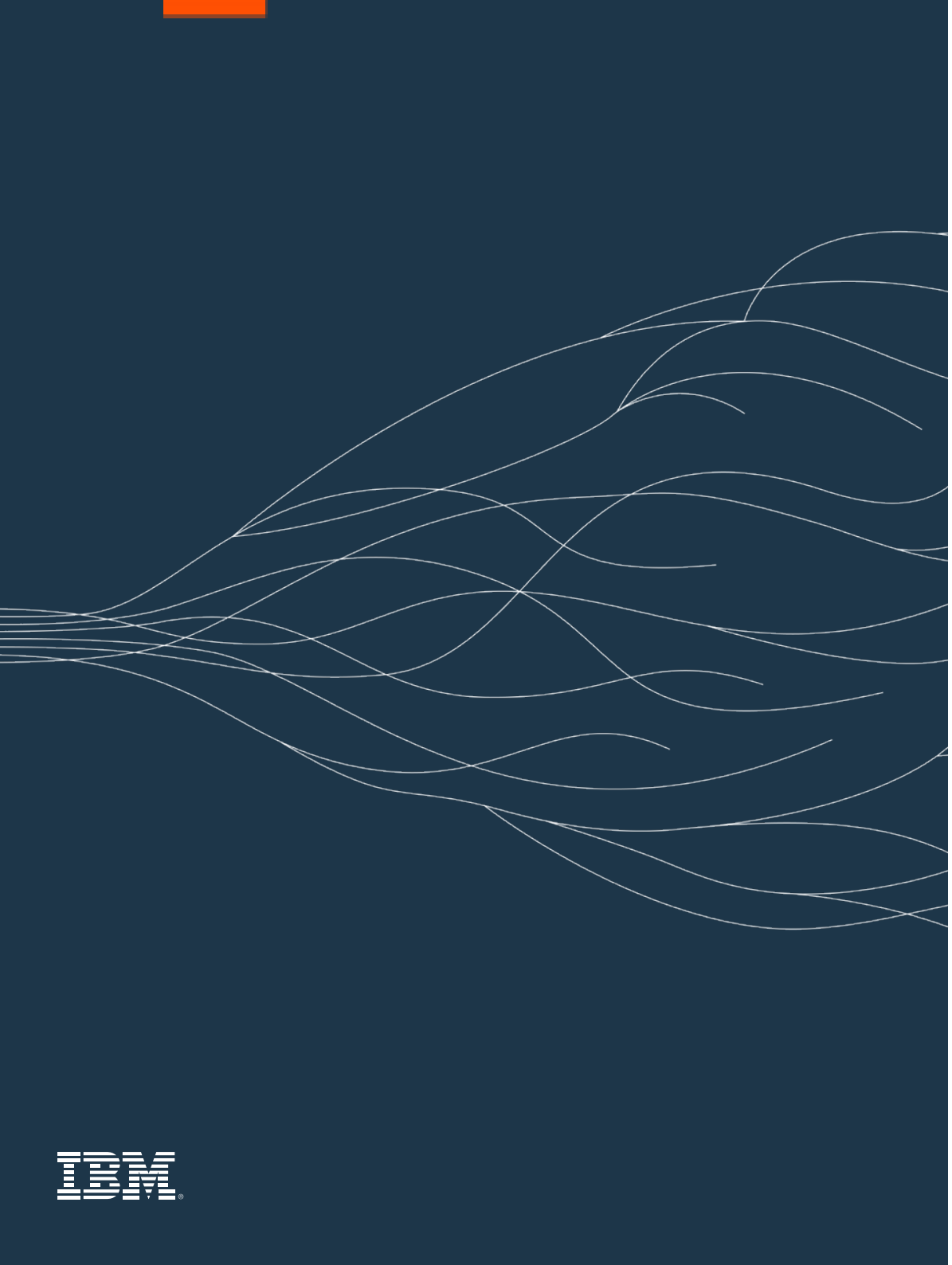

IBM Security

# 零售行业安全趋势

## 攻击者瞄准唾手可得的成果

**IBM X-Force 研究**

IBM

单击此处开始 ▶

# 目录

要点概述
1 • 2

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



## 要点概述

尽管某些广为人知的攻击类型针对的是大型零售商，但 2015 年网络犯罪分子开始将其目标从大型零售商转向小型企业。我们怀疑 2016 年这种情况仍将继续，但行业分析师难以评估问题的真实程度，因为许多小型零售商可能并未报告攻击情况。这一趋势应波及大型企业，因为攻击者可能会将小型企业视为通过供应链或支付门户攻击目标大型企业的路径。

IBM® Managed Security Services (IBM MSS) 数据显示，今年的 Shellshock 攻击率很高，占 IBM MSS 客户端网络中发现的威胁活动 1/4 以上，在 Shellshock 爆发 2 周年之际（9 月[1]和 10 月[2]），攻击活动明显增加。长期以来，SQL 注入和暴力攻击深受网络犯罪分子的欢迎，因为它们的成功率已经得到证明，是第二和第三种最常见的攻击类型。作为用来被动收集关于目标系统信息以识别漏洞的预攻击手段，指纹识别占据近 11% 的攻击活动。

Ponemon 2016 数据泄露成本研究：全球分析显示，对零售商带来的经济损失将持续上升。2015 年，零售行业的数据成本显著增加，从 2014 年每条记录 105 美元增加到 2015 年的 165 美元。2016 年，这一数字上升至每条零售记录 172 美元，远高于 158 美元的跨行业平均成本。

随着购物季的全面展开，我们还评估了黑色星期五/网络星期一周末的攻击数据。这似乎是攻击增加的好时机，但从历史上看，我们尚未发现 IBM MSS 客户端网络上的威胁活动急剧上升。今年的表现并无不同，针对零售商的每日平均攻击次数略低于全年的日平均值。

## 目录

要点概述
1 • 2

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



值得注意的是，攻击活动的这一趋势并不能体现信用卡欺诈的发生频率。事实上，一份报告显示，2016 年黑色星期五到网络星期一的在线零售信用卡欺诈率比 2015 年高出 20%。[3] 去年的 IBM 零售报告强调了密码芯片卡与签名芯片卡的安全性，但芯片卡的出现明显未解决信用卡欺诈问题。它甚至引入了晦涩的法律条文，一些美国大型零售商向信用卡公司提起诉讼，要求他们允许使用签名芯片卡。[4] 鉴于困扰零售行业的这些问题，组织需要了解这种趋势，进行最适合自身的安全性投资。我们的建议旨在优化安全性计划，以阻止高级威胁，保护零售行业的“重要资产”。

### 关于 X-Force

IBM X-Force 研究团队负责研究和监控最新的威胁趋势，包括弱点、漏洞、攻击、主动攻击、病毒及其他恶意软件、垃圾邮件、网络钓鱼和恶意网络内容。除了向客户和公众提供有关新兴和关键威胁的建议外，IBM X-Force 还提供安全内容以保护 IBM 客户免受这些威胁。威胁情报内容直接通过 IBM X-Force Exchange 协作平台提供，请访问：xforce.ibmcloud.com

IBM Security

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物
而非攻击

建议

保护企业的同时降低成本
和复杂性

关于 IBM Security

关于作者

参考资料

## 个性化、隐私与安全的交集

消费者往往同时寻求提高零售帐户的个性化和隐私性，但有时也会混淆隐私与安全。在不损失隐私性的情况下难以实现个性化，而隐私与安全并不相同。

在数据收集方面，隐私是指信息的安全收集以及公司对此等信息的适当存储和使用。这种信息收集支持消费者帐户个性化。例如，消费者可提供人口统计信息以便接收适合其年龄、性别等方面的广告和优惠券。很多人愿意提供这些细节；去年发布的一项全球调查发现，54% 的消费者可能会与零售商分享信息。[5]

随着零售商寻求通过跟踪和整合来自各种设备（如智能手机、平板电脑和销售点 (POS) 系统）的数据来全面实施个性化，客户体验变得更加无缝和愉悦。但零售商收集和整合的数据越多，就越容易受到攻击。零售已成为主要攻击目标，随着数据存储库的增长，它提供了一个对犯罪分子更有吸引力的数据丰富的环境。

为了解决隐私问题，零售商应提供易于理解的隐私政策来保持透明度，并让消费者有权选择何时以及如何收集和使用他们的数据。消费者还应该明白，他们的很多数字互动都会留下数据痕迹，一定程度上，在个性化和隐私之间找到适当的平衡是他们自身的责任，而不仅仅是零售商的责任。

零售商的任务是从隐私和安全的角度保护消费者的敏感信息。即使企业妥善收集、存储和使用信息，也必须关注下一节中讨论的攻击类型，并设法减少消费者数据渗漏。

IBM

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击
1 • 2 • 3

零售行业的趋势

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



## 针对零售行业的普遍攻击

IBM Managed Security Services 每年监控 100 多个国家/地区的客户端设备报告的数十亿起事件，分析了我们在 2016 年 1 月 1 日至 2016 年 11 月 30 日期间积累的汇总数据。这些数据对零售行业面临的日常网络体验提供了洞察。

在本节中，我们将攻击定义为在系统或网络中发现的安全事件，此事件已被关联和分析工具确认为试图收集、破坏、拒绝、降级、伪造或破坏信息系统资源或信息本身的恶意活动。

前五大攻击媒介 - Shellshock、SQL 注入、暴力攻击、指纹识别和后门程序 - 占针对零售行业实施的攻击活动的 74% 左右。图 1 细分了最普遍的攻击媒介。

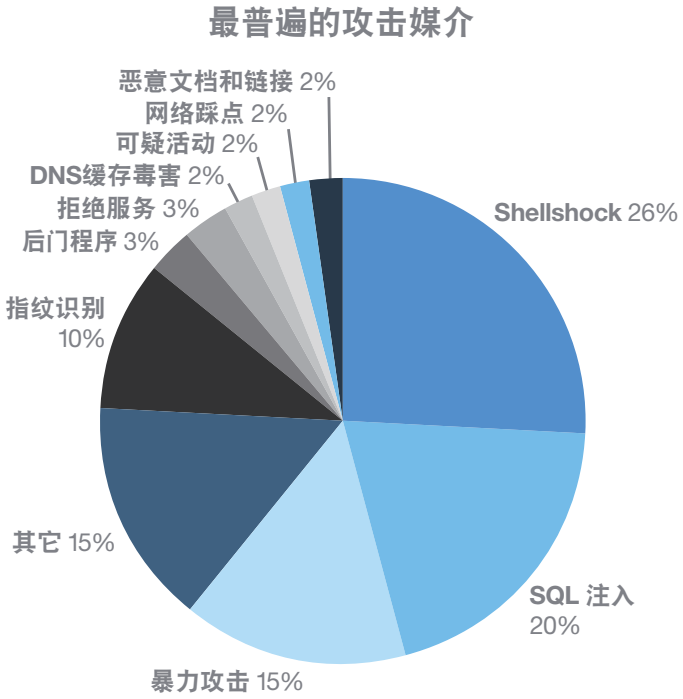


**图 1.** 零售行业最普遍的攻击媒介。（2016 年 1 月 1 日 - 2016 年 11 月 30 日）。来源：IBM Managed Security Services 数据。

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击
1 • 2 • 3

零售行业的趋势

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料

IBM Security

### Shellshock

不出所料，Shellshock 是排名第一的攻击媒介，占所有攻击活动的 26%。Shellshock 是 Linux、Solaris 和 Mac OS 系统中广泛使用的 GNU Bash shell 中的漏洞。2016 年 9 月 24 日是这一威胁爆发两周年的纪念日，它制造了 2014 年信息安全领域最轰动的头条新闻之一。仿佛是预计到其周年纪念日一样，Shellshock 袭击活动在 9 月飙升至 2015 年以来的最高水平。10 月份出现了第二波攻击狂潮。[6] 鉴于这种激增现象，2016 年零售行业遭遇的 Shellshock 攻击数量几乎是 2015 年的两倍，其中 60% 发生在 9 月份，这一点不足为奇。

### SQL 注入

SQL 注入是针对零售商的第二大攻击媒介，占 20% 的攻击。薄弱的 SQL 数据库安全策略是攻击成功的共同特征。具有讽刺意味的是，IBM X-Force 漏洞数据库的数据显示，虽然利用此威胁的攻击仍然很普遍，但近几年披露的 SQL 注入漏洞数量大幅下降，而相关漏洞利用代码已对公众开放。事实上，从 2011 年到 2015 年，披露的 SQL 注入漏洞数量下降了 54%。漏洞与公开可用的漏洞利用代码比率也在下降。这意味着攻击者只对未修补的较旧 SQL 注入漏洞成功实施了攻击。


2016 年零售商经历的超过一半的 Shellshock 攻击都发生在 9 月份，即 Shellshock 爆发的周年纪念日。

IBM

IBM Security

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击
1 • 2 • 3

零售行业的趋势

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料

### 暴力攻击

暴力攻击占 15% 的攻击。暴力密码攻击是一种入侵者试图猜测用户名和密码组合以非法访问系统或数据的策略。发现的大多攻击都是针对 Secure Shell (SSH) 服务。攻击者之所以偏爱 SSH，是因为它提供了跨网络的 Shell 帐户访问。

### 指纹识别

超过 10% 的攻击涉及到指纹识别，通常被视作预攻击，用于收集有关潜在目标的信息并寻找其中存在的弱点。本质上，攻击者将目标系统的输出与已知的“指纹”进行比较，这些指纹唯一标识有关目标的特定详细信息，比如操作系统或应用程序的类型或版本。攻击者可通过此信息利用目标组织的 IT 基础架构中的已知漏洞。

### 后门程序

3% 的攻击涉及到某些 TCP 端口上的请求，这些请求表明攻击者正在受到攻击的网络上运行后门程序。后门程序可使攻击者绕过安全验证机制访问计算机程序。大多数后门程序是通过系统漏洞（如病毒或蠕虫）部署在系统上的。

IBM

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势
1 • 2 • 3

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



# 零售行业的趋势

## 尽管出现了积极的信号，但来自 POS 恶意软件的威胁仍持续存在

POS 恶意软件旨在提取客户支付卡数据，并发回给由攻击者控制的命令与控制 (C&C) 服务器，2013 年 12 月之前主流媒体对此鲜有提及。在史上规模最大、曝光度最高的一次数据泄露事件中，超过 1 亿张信用卡卡号从美国零售连锁店被盗。[7] POS 恶意软件病毒在 2014 和 2015 年发展势头强劲，多起信用卡泄露事件导致高端零售品牌受损，其功能也不断增加：整合僵尸网络功能、与中央命令与控制服务器通信、在受感染的系统上部署键盘记录程序、利用创造性的渗漏方案将数据发给攻击者。[8]

鉴于这一威胁似乎在两年间愈演愈烈，故此我们想评估其在 2016 年的影响力。有趣的是，IBM MSS 数据显示，去年排名前列的攻击媒介（使用恶意文档和网站）今年排名很低，仅占攻击活动的 2%（见图 1）。攻击旨在欺骗受害者打开恶意文档或点击恶意网站的链接，几乎总是试图让受害者下载恶意软件。就零售商而言，恶意软件通常是基于 POS。

攻击活动减少可能表明更多零售商在实施保护 POS 系统的最佳实践，比如限制互联网访问和更新软件。因此，攻击者发现这种威胁媒介的吸引力越来越小。

除了 IBM MSS 数据显示的这一观察结果外，我们也从另一份报告中发现[9]，2016 年针对 POS 系统的新恶意软件变体越来越少。新变体减少意味着安全供应商能更及时地应对威胁，降低零售商面临的风险。

目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势
1 • 2 • 3

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



这是否意味着 POS 恶意软件不再是重大威胁？不，远非如此。虽然利用恶意文档和链接的新恶意软件变体和攻击现象减少令人鼓舞，但威胁仍然存在。今年报告了几起 POS 恶意软件事件，其中一起针对的是一家知名度较高的娱乐产业组织，在近一年的时间里未发现恶意软件[10] - 这只是 2016 年发生的几起事件之一，攻击者在长达三个月到一年的时间里肆意收集未检测到的数据。正逢假期之际，我们发现了新的 POS 恶意软件系列 ScanPOS，其通过新的网络钓鱼活动进行分发。[11] 因此，我们采取谨慎的态度，并强烈建议您应用我们在本报告末尾提供的保护 POS 系统的建议。

## 勒索渗透到零售行业

勒索软件和其他勒索攻击所带来的风险越来越受到各个行业的关注。零售行业也不例外。过去几年中，零售勒索软件事件层出不穷。2014 年，一家国际披萨连锁餐厅 65 万比利时和法国客户的个人资料在勒索未遂后被泄露。[12] 在今年一起引人注目的事件中，一家美国餐厅遭到勒索软件攻击，攻击者索取 1 万美元才会解锁加密文件。[13] FBI 通知该餐厅，这是海外网络犯罪分子锁定的八家企业之一。在另一次勒索攻击中，某韩国电子商务门户网站超过 1000 万客户的姓名、地址和电话号码被盗。[14] 勒索者要求用 266 万美元的比特币换取公司数据。

随着 2016 年底新的 POS 恶意软件系列崛起，零售销售点系统作为窃取信用卡数据的工具仍易受到攻击。

目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势
1 • 2 • 3

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



### 零售和物联网

智能手表和恒温器等物联网 (IoT) 设备今年可能会出现在消费者的假日购物清单上，但攻击者对此类设备可能制定了其他计划。近期对域名提供商 Dyn 实施的破纪录的分布式拒绝服务 (DDoS) 攻击采用 Mirai 物联网僵尸网络，让人们注意到物联网设备越来越容易受到攻击。[15]

电信当然不是唯一受到攻击的行业。6 月份，安全研究人员发现超过 25,000 台闭路电视摄像头被用来对美国一家小型珠宝店网站实施为期数天的 DDoS 攻击。[16] 零售商的网站不仅容易受到物联网僵尸网络的攻击，而且实体店中安装的闭路电视摄像头也会受到攻击，并被物联网僵尸网络用来攻击其他目标。网络中日益增加的物联网设备通常无法获得新计算机的安全审查级别，因此它们更容易成为多种攻击类型的攻击目标。

在零售领域，物联网具有多种新的用途，比如检测购物者在商店中的位置和行为。[17] 利用和分析此类信息有助于零售商为消费者提供更智能的购物体验。但如果我们不在这些应用程序中构建安全性，很可能会对零售商和客户产生负面影响。此外，供应链中物联网的存在创造了几乎完全可见的可能性，因为从制造商到消费者的所有数据都会经过分析。可见性增强为零售商提供了可执行信息，用以提高效率，从而降低成本。但缺点是物联网设备通过易受攻击的应用程序编程接口 (API) 进行通信，因而攻击面增大。只要攻破一个物联网设备，攻击者便有可能访问多个组织的网络并渗漏数据或注入恶意软件。

IBM Security

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击
1 • 2

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料

## 攻击者是在购物而非攻击

攻击者利用节假日之便，通过垃圾邮件、网络钓鱼和受到攻击的网站发起攻击，在一年中的这个时候，恶意假日主题活动数量必将增加。在近期一次垃圾邮件活动中，这些电子邮件被伪装成信誉良好网站的官方“黑色星期五交易”，试图用礼品卡代码欺骗受害者。另一次恶意活动利用了 Locky 勒索软件，在由 IBM Security 分析的所有传入垃圾邮件中，高峰时期它占据其中 72%。[18]

然而，令人惊讶的是，近年来的 IBM Security 研究显示，在黑色星期五/网络星期一期间针对零售行业的攻击未显著增加。今年，黑色星期五和网络星期一期间的流量似乎急剧增加，但在四天的延长周末，攻击次数实际上低于全年的日平均值（见图 2）。

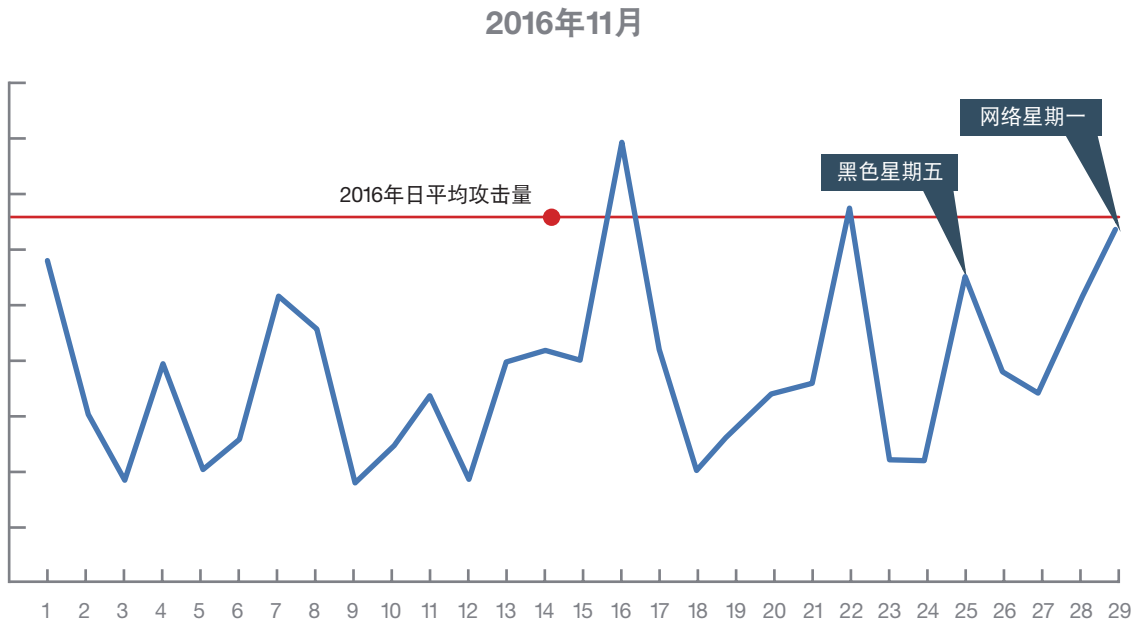


**图 2.** 黑色星期五到网络星期一期间的零售商每日平均攻击次数低于全年的日平均值（2016 年 11 月 1 日 - 2016 年 11 月 29 日）。来源：IBM Managed Security Services 数据。

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击
1 • 2

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



当然，节假日期间会出现严重的漏洞和猛烈的攻击。在此期间，每日安全攻击量可能低于预期，因为网络犯罪分子可能会在今年早些时候实施犯罪活动，为在假日购物狂潮期间攫取利益打下基础。攻击者经常渗透系统，在发布任何公告或在目标组织发现漏洞之前，花费几个月的时间秘密收集数据。

用户教育也有可能产生积极影响。节假日期间会有很多警告，用户实际上可能比平时更加警惕，并且在点击假日电子卡中跳舞的圣诞老人之前会犹豫再三，这种电子卡会安装恶意软件，或通过闪烁的“折扣”图像诱使他们访问恶意网站。旺季保持额外的警惕也可能是攻击次数减少的原因。为什么要在众目睽睽之下实施攻击?

黑色星期五“交易”，在电子卡中跳舞的圣诞老人和闪烁的“折扣”图像可能是以假日为主题，试图让用户点击恶意链接或下载恶意软件。

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击

建议
1 • 2

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



# 建议

针对零售行业的攻击者对攻击网站兴趣不大，而是将更多注意力放在获取有价值的信息上，比如信用卡数据。这与其他行业攻击者的动机有很大不同，在这些行业中，破坏可能更有激励性。此外，零售行业攻击者利用 SQL 注入和暴力攻击这样久经验证的可靠媒介对需要基本保护的组织实施攻击。

## 先从基础开始：识别、保护、检测和恢复

虽然大型零售商容易遭到 SQL 注入和暴力攻击，但小型零售商更有可能成为受害者。这些媒介所针对的漏洞可被视作唾手可得的成果，且在未采取基本安全措施（识别、保护、检测和恢复）的小型企业环境中很常见。大型企业应予以关注，因为攻击者可能会将小型企业视为通过供应链或支付门户攻击目标大型企业的路径。问题往往在于中小型企业可能不确定何处以及如何着手解决网络安全问题。在美国，可在美国国家标准与技术研究院 (NIST) 指南小企业信息安全：基本知识中找到有关问题的帮助。理想情况下，各种规模的业务和企业都应采用以下最低限度的建议。

## 网络可见性

对网络事件的可见性至关重要。安全信息和事件管理 (SIEM) 工具可为各种规模的组织提供预防、检测和响应最新威胁的有效方法，以免造成破坏。分析网络流量以实时识别安全威胁是确定安全事件优先级的关键。诸如 IBM QRadar Security Intelligence Platform 之类的工具整合了分布在整个网络中的数千个设备、端点和应用程序的日志事件和网络流量数据。

## 漏洞修补

两大攻击媒介 Shellshock 和 SQL 注入会利用未修补的漏洞，所以及时的补丁管理对于任何规模的组织都至关重要。通过从安全情报和数据分析工具（如 IBM Qradar 和 IBM BigFix 端点管理解决方案）收集的分析，您需要确定自己所在行业的重大漏洞，并始终（是始终！）对系统进行修补和更新。

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击

建议
1 • 2

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料



### 缓解暴力攻击

如今许多产品和服务都需要强密码，但弱密码仍能帮助犯罪分子成功实施暴力攻击。强制使用不允许出现在常见密码列表中的字词的强密码。在三到五次登录尝试失败后锁定帐户。对各类失败登录返回的错误消息相同，因此攻击者无法判断是否使用了有效的用户 ID 却输入了错误的密码，反之亦然。不允许直接登录管理员帐户。有关其他建议，请查看 IBM 报告小心旧式网络攻击。

### 保护 POS 系统

来自 POS 恶意软件的威胁似乎略有减少，但零售组织仍应保护其针对 POS 恶意软件的端点销售机制。至少，我们强烈建议实施去年的零售行业报告中所列的最佳实践。

## 保护企业的同时降低成本和复杂性

从基础架构、数据和应用程序保护到云和安全管理服务，IBM Security Services 拥有专业的知识，可以为贵公司的关键资产保驾护航。我们能为世界上最复杂的网络提供保护，并雇佣业内最优秀的人才。

IBM 提供的服务可帮助您优化安全计划、阻止高级威胁、保护数据并保障云和移动的安全。Security intelligence Operations and Consulting Services 可以根据安全方面的最佳实践评估您的安全状况和成熟度。凭借 IBM X-Force Incident Response and Intelligence Services，IBM 专家可主动搜索和响应威胁，并在攻击发生之前应用最新的威胁情报。借助 IBM Managed Security Services，您可以利用业界领先的工具、安全情报和专业知识，来帮助您改善安全状况 - 成本通常只占内部安全资源的一小部分。

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料

IBM Security

## 关于 IBM Security

IBM Security 可提供最先进的集成式企业安全产品和服务组合之一。该组合以世界知名的 IBM X-Force 研究为后盾，提供充足的安全智能，借助身份和访问管理、数据库安全、应用程序开发、风险管理、终端管理、网络安全及其他各方面的解决方案，帮助企业全面保障其人员、基础架构、数据和应用程序的安全。IBM 拥有世界上规模最大的安全研发和交付机构，每天监控 130 多个国家超过数十亿起安全事件，并持有 3,500 多项安全专利。

## 关于作者

Michelle Alvarez 是 IBM Managed Security Services 的威胁研究员和编辑，她在工作中融入了自己 10 多年的从业经验。Michelle 负责研究和分析安全趋势，撰写并编辑安全和威胁缓解思想领导力论文。她于 2006 年通过 Internet Security Services (ISS) 收购加入 IBM。在 ISS，她担任分析师，并为世界上最全面的威胁和漏洞数据库之一 - X-Force 数据库的开发做出了贡献。多年来，Michelle 在信息技术 - 信息共享和分析中心 (IT-ISAC) 发挥着举足轻重的作用，该公司是由信息技术部门成员组成的非营利性有限责任公司。她是 IBM 赞助的安全博客 SecurityIntelligence.com 的定期撰稿人，并拥有信息技术硕士学位。

## 撰稿人

Scott Craig – IBM Security 威胁研究员

## 了解更多信息

要了解有关 IBM Security 产品组合的更多信息，请联系 IBM 销售代表或 IBM 业务合作伙伴，或者访问：**ibm.com**/security

有关安全服务的更多信息，请访问：**ibm.com**/security/services

请关注我们的 Twitter：@IBMSecurity，或者访问 IBM 安全情报博客

IBM

IBM Security

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料

## 参考资料

1 *https://securityintelligence.com/shellshock-anniversary-major-security-flaw-still-going-strong/*

2 *https://securityintelligence.com/researchers-detect-second-wave-shellshock-attacks-since-two-year-anniversary/*

3 *http://www.darkreading.com/analytics/holiday-weekend-online-payment-card-fraud-20--higher-in-2016-/d/d-id/1327610*

4 *http://www.bankrate.com/finance/credit-cards/how-lawsuits-over-chip-and-pin-affect-consumers.aspx*

5 *https://www.sas.com/content/dam/SAS/en_us/doc/research1/balance-between-personalization-privacy-107399.pdf*

6 *https://securityintelligence.com/researchers-detect-second-wave-shellshock-attacks-since-two-year-anniversary/*

7 *http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/*

8 *https://securityintelligence.com/the-pos-malware-epidemic-the-most-dangerous-vulnerabilities-and-malware/*

9 *http://www.eweek.com/security/pos-malware-declines-as-spam-volume-grows-sonicwall-reports.html*

10 *http://notice.themadisonsquaregardencompany.com/customerupdate/*

11 *http://www.morphick.com/resources/lab-blog/scanpos-new-pos-malware-being-distributed-kronos*

12 *http://www.theguardian.com/technology/2014/jun/16/dominos-pizza-ransom-hack-data*

13 *http://www.wusa9.com/news/local/rockville/scam-artists-hack-restaurant-computer-demand-10k/102424542*

14 *http://www.koreatimes.co.kr/www/news/nation/2016/07/116_210566.html*

15 *http://www.fiercetelecom.com/telecom/dyn-confirms-friday-ddos-attack-was-based-mirai-botnet*

16 *https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html*

17 *https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=AB&infotype=PM&htmlfid=WWC12356USEN&attachment=WWC12356USEN.PDF*

18 *https://exchange.xforce.ibmcloud.com/collection/Amazon-Cyber-Week-Spam-Campaigns-c2ad3c53d2e3a5432024a6a137ab233c*

IBM

## 目录

要点概述

个性化、隐私与安全的交集

针对零售行业的普遍攻击

零售行业的趋势

攻击者是在购物而非攻击

建议

保护企业的同时降低成本和复杂性

关于 IBM Security

关于作者

参考资料

IBM Security

IBM Security
Route 100
Somers, NY 10589

美国印制
2016 年 12 月



IBM

SEL03121-CNZH-00