IBM Security

制造业的安全趋势

知识产权和运营信息都是“皇冠上的宝石”

IBM X-Force® Research

IBM

点击此处开始 ▶

IBM Security

目录

执行概要

首先来说个好消息：根据 IBM® Security Services 的监控结果，制造业客户在 2016 年遭受的攻击要少于所有其他行业的客户。再来说个坏消息：制造业中所遭受的“安全意外事件”（即属于最严重分类的安全攻击事件）所占的比例比其他所有行业的平均比例几乎要高出 40%（见图 1）。总体来说，根据 2017 年 IBM X-Force 威胁情报指数披露，制造业是 2016 年按受攻击次数排序位列第三的领域。

尽管制造领域的安全意外事件数量要高于各个行业的平均水平，但在 2016 年，制造领域所遭受的**攻击次数和安全意外事件数量**同比**都有了大幅下降**。就所有行业而言，从 2015 年到 2016 年，这些数据也有大幅下降：攻击次数下降了 12%，安全意外事件的数量下降了 48%。

制造领域的下降幅度同样很大：攻击次数下降了 38%，安全意外事件的数量下降了 53%。

术语定义

安全事件：安全设备或安全应用检测到的发生在系统或网络中的活动。

攻击：关联和分析工具将其识别为试图收集、扰乱、摒弃、恶化或毁坏信息系统资源或信息的恶意活动的安全事件。

安全意外事件：经 IBM 安全分析师审查且被视为值得进一步调查的安全意外事件的攻击和/或安全事件。

图 1. IBM 在 2016 年监控的组织对比（各个行业的客户与制造业客户）。（有关“安全事件”、“攻击”和“安全意外事件”的定义，请参见侧边栏的“术语定义”部分。）来源：IBM Managed Security Services 数据，2016 年 1 月 1 日至 12 月 31 日。

目录

IBM Security

制造领域值得关注的已公开意外事件

由于 2016 年制造领域公开披露的意外事件非常少，因此据 IBM X-Force 研究员的猜测，可能有一些意外事件并未报告，这或许是因为制造业的监管力度或审查力度并没有金融服务、医疗保健和零售业等行业那样严苛。尽管如此，仍旧有些值得关注的意外事件进行了公开披露，比如全球最大的钢材制造商之一的商业机密在这一年里遭到了网络盗窃事件。[1]

在制造商眼中，知识产权 (IP) 和内部运营信息 (OI) 都犹如“皇冠上的宝石”般珍贵，因此并不会像现金或个人身份信息那样容易被忽略，但网络犯罪分子和商业间谍交易商依然对其虎视眈眈。

攻击者会利用各种机会，采用已经在其他行业得到验证的攻击战术实施攻击。其中一种方式就是使用商业邮件攻击 (BEC) 诈骗，包括全球电汇诈骗攻击，这类攻击的目的是攻击公司高管的合法商业电子邮件帐户，让他们的员工进行未经授权的电汇操作。[2]

关于本报告

本 IBM X-Force 研究报告 IBM Managed Security Services 威胁研究小组编写，该小组由经验丰富、技能熟练的安全分析师组成，致力于及时向 IBM 的客户通知最新的网络犯罪威胁，使他们做好充分准备。该研究团队分析了来自多个内部/外部来源的安全数据，包括来自由 IBM 托管并监控的终端设备的安全事件数据、活动与趋势。

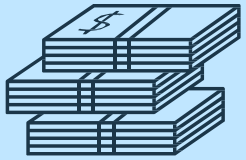
IBM

IBM Security

BEC 诈骗攻击也会以员工的纳税数据为目标，然后利用这些数据获得欺诈回报并在暗网市场上出售。2016 年 4 月，一家船用电动机与供货公司披露其遭受了 BEC 诈骗攻击：该公司的一名员工不经意将所有员工的 W-2 表格提供给了一个未经授权的第三方。[3] 此类意外事件的成本非常高昂：每条丢失或被盗记录都包含有敏感的机密信息，平均泄露成本高达 156 美元；因此制造商均应尽最大努力阻止可能会造成数据泄露的一切威胁。

在 2016 年，制造业也未能幸免；在这一年，勒索软件和数字勒索几乎在每个行业、每个地区都找到了立足点。[4] 在一次意外事件中，一家与美国海军有业务往来的预浇筑混凝土与建筑服务公司成为了攻击者的目标，攻击者威胁称，如果该公司不支付赎金的话，他们就会出售盗窃获得的数据。[5] 还有一家聚氨酯和环氧树脂产品制造商也遭到了相同的威胁：支付赎金，否则我们就会出售盗窃到的数据。[6]

威胁形势刻不容缓。勒索软件传播的速度和步伐非常快，尤其是勒索软件即服务 (RaaS)[7] 也已出现，因此，制造商应采取一切可能采取的措施做好有效的响应准备。



投机型攻击者使用电子邮件诈骗、勒索软件和数字勒索等手段从制造商处骗取金钱。

IBM Security

"坏家伙"在哪里？内部人员与外部人员

安全主管及其团队每年都会解决多起攻击事件，也将会持续监视威胁来源，以便对其防御措施和预算进行优先排序。安全调查团队的第一步是识别源 IP 和目标 IP 来自于内部还是外部，然后进一步调查相关的攻击模式，以确定攻击事件属于恶意性质还是由于疏忽所致。

这些天他们有什么发现？大多数攻击者是外部人员吗？或者说其组织遭受的大部分攻击来自于内部人员？

据 IBM Managed Security Services 2016 年的监控数据（见图 2）披露，外部人员攻击的数量 (91%) 要远远高于内部人员攻击 (9%)；而在内部人员攻击中，由于疏忽造成的攻击数量 (5%) 略高于恶意内部人员的攻击数量 (4%)。

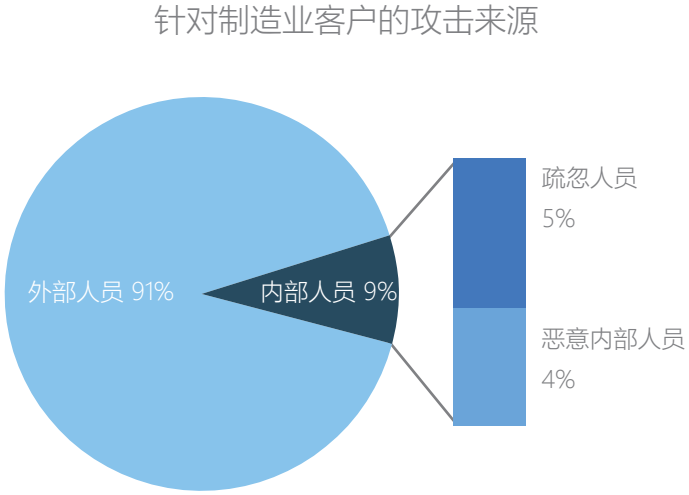


图 2. 2016 年，制造业遭受的外部人员攻击数量要高于内部人员攻击。

来源：IBM Managed Security Services 数据，2016 年 1 月 1 日至 12 月 31 日。

据 2017 年 IBM X-Force 威胁情报指数披露，在遭受攻击最多的五个行业中，还有两个行业遭受的外部人员攻击数量高于内部人员攻击，分别是零售业和信息/通信业。

外部人员包括资金充裕的黑客、有组织的犯罪集团和民族国家攻击者。制造领域遭受的大多数外部人员攻击都是采用 SQLi 和 CMDi 等注入式攻击机制发起的。

IBM

制造领域受监控客户端中的主流攻击方法

为了澄清并更好地了解会对制造商造成影响的威胁类型，IBM X-Force 按照依据 MITRE Corporation 的 CAPEC™（常见攻击模式枚举与分类）制定的标准对其在 2016 年监测到的攻击类型进行了分类（见图 3）。

据 MITRE 的介绍，他们的系统“会根据攻击者在漏洞利用方面经常使用的攻击机制分层次地组织攻击模式”。唯一的例外就是“指示器 (Indicator)”类别，该类别的作用是描述威胁与攻击模式的条件和情境信息。

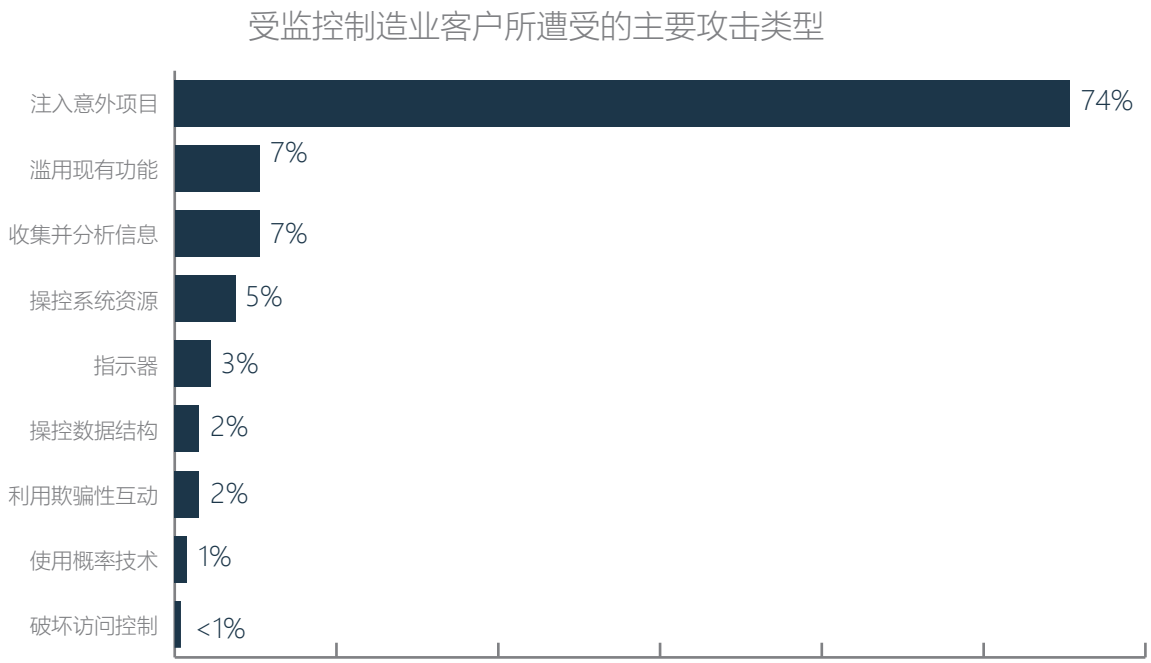


图 3. 注入式意外事件几乎占到制造业 2016 年所遭受全部攻击类型的四分之三。来源：IBM Managed Security Services 数据，2016 年 1 月 1 日至 12 月 31 日。

以下章节将针对每个攻击类型进行更详细的介绍。

注入意外项目

IBM Managed Security Services 对 2016 年所遭受攻击的分析结果显示，排名第一的攻击类型是使用恶意输入数据来尝试控制或扰乱系统；在 IBM X-Force 监控的制造业客户中，有 74% 的客户遭到了此类攻击。该项数据远远高于其他行业所遭受此类攻击的占比 (42%)。

命令注入（包括操作系统命令注入 (OS CMDi) 及 SQLi）即属于这个类型的攻击。SQLi 攻击在所有攻击类型中的占比为 45%。OS CMDi 攻击的占比是 18%，这类攻击又被称作"外壳命令注入"，目前臭名昭著且广泛盛行的"破壳"漏洞也是以此命名。[8] 另外还有 11% 的攻击采用的是其他类型的注入方法。

这些监控结果表明，攻击者往往选择运行过时的 SQL 服务器的制造商为攻击目标。举例来说，针对 SQL Server 2005 的支持已于 2016 年 4 月停止。[9] 对于仍在运行 SQL 2005 的企业而言，如果不升级的话，就可能会存在严重的安全漏洞。

滥用现有功能

排名第二的攻击类型是攻击者尝试滥用或操控"应用的一个或多个功能，以将某个资源全部投入到会使目标的功能受到影响的某个点上。[10] 此类攻击在制造业中的占比是 7%，高于其他行业客户的平均占比 (2%)。

在受监控制造企业所遭受的攻击中，有四分之三的攻击属于以数据库 (SQLi) 和操作系统 (OS CMDi) 为目标的注入式攻击。

收集并分析信息

攻击者还会采用收集并盗窃客户端设备信息的方式进行攻击，此类攻击类型的占比为 7%。大多数此类攻击都与数字指纹有关，通常这种攻击被视为一种侦查方式，旨在收集潜在目标上的信息，以发现其中的现有漏洞。从根本上来说，攻击者会对来自目标系统的输出与用于识别目标相关特定详情（诸如操作系统或应用的类型或版本）的已知“指纹”进行对比。攻击者能够使用这些信息识别目标组织 IT 基础架构中的已知漏洞并完善他们的战术计划。

操控系统资源

攻击者还会尝试操控系统资源的状态或可用性，这种攻击类型的占比是 5%。这种资源包括文件、应用、库以及配置信息。在这种攻击类型中，攻击者一旦成功，便会导致服务拒绝，将目标机器感染为僵尸网络的一部分，授权攻击者访问公司的网络或在目标上执行任意代码。

指示器

请注意“指示器”并不属于 CAPEC™ 攻击机制。网络威胁指示器由特定的可观测条件及有关条件或模式的情景式信息构成。此类“指示器”类型的攻击事件（占比 3%）能够指示目标系统上的尝试攻击或成功攻击。大部分此类攻击的目标系统会首先在短时间内遭到 100 次或以上的外部定位，这可能指示内部主机已受到危害。如果主机受到危害，主机可能会无意地攻击其他目标，或与其他受危害的主机进行通信，直至被检测到并被制止为止。

操控数据结构

此类攻击在其他行业中的占比高达 32%，而在制造服务领域，此类攻击的占比非常低，只有 2%。这可能是因为攻击者认为此类攻击在制造领域取得成功的可能性较小。此类攻击是指攻击者通过操控系统数据结构来尝试获得非授权访问权限。正如 CAPEC™ 中所述，“通常而言，由于系统设计及其预期处理过程中的模糊性和假设，会导致系统中存在着许多漏洞［诸如缓存溢出漏洞］，进而导致其数据结构也可供攻击者所用。”[11]

IBM Security

利用欺骗性互动

此类攻击的占比是 2%；在此类攻击中，攻击者会尝试通过电子欺骗的方式劝诱受害者执行某项操作，比如点击劫持或用户界面伪装攻击。在此类攻击中，攻击者会尝试劫持受害者的点击操作，而且可能会发起进一步攻击。计算机并非唯一目标。近期发布的一篇报告特别指出，安装 Android 系统的移动设备在使用 Google Play 应用时容易遭受点击劫持的攻击。

使用概率技术

在所有攻击中，占比为 1% 的攻击类型是：攻击者使用 CAPEC™ 中所述的“概率技术探索并攻克目标的安全属性。”[13] 大部分此类攻击都涉及暴力密码破解攻击，在这种攻击中，入侵者会尝试猜测用户名与密码组合，以获得系统或数据的非授权访问权限。据 IBM X-Force 的监测，大部分此类攻击的目标都是安全外壳 (SSH) 网络协议。用户之所以偏爱使用 SSH 服务，是因为该服务能提供安全的远程访问。该服务的劣势在于它能够为攻击者提供网络中的外壳帐户访问权限。

破坏访问控制

此类攻击是指攻击者尝试“利用目标管理身份与授权时所用的机制中的漏洞、限制事项和假设事项[14]”破坏访问控制，其占比不到 1%。在大多数此类攻击中，攻击者会利用服务器向有效客户端给予的默示信赖，攻击目标系统客户端与服务器之间用于鉴定与数据完整性验证所用的通信通道中的漏洞。

此类攻击还包括中间人 (MITM) 攻击，即攻击者尝试拦截并转发两方（人员或系统）之间的消息。通过这种技术，攻击者可以获得往来信息的访问权限和/或盗取往来信息，或者在连接中插入恶意代码。

IBM

IBM Security

建议与减缓措施

安全的生产环境和可信的供应链是制造商专有信息与产品安全保护的关键。根据本报告的调查结果，我们为制造商提出了以下几点最佳实践指南。

采用集中式的补丁修复，维持数据输入“卫生”

在针对制造业的攻击中，排名第一的攻击类型是使用 SQLi 或 CMDi 等恶意输入数据。若要减缓此类攻击，对当前的软件版本进行补丁修复和维护非常关键。在这一方面，管理员遭遇的难题是需要针对成千上万台终端设备的多个操作系统和应用进行补丁管理和部署。幸运的是，制造企业可以采用 IBM BigFix® Patch Management 解决方案自动完成并简化补丁修复流程。

除了及时修复补丁之外，输入数据的控制与“卫生”也是减缓注入式攻击的重要步骤之一。攻击者可以采用多种方式利用“不卫生”的输入数据发起攻击，因此必须全面维护数据卫生。总而言之，要对所有用户输入进行过滤。

终端设备检测与响应

通过高效的终端设备检测与响应解决方案来确保网络可视性，可帮助您快速识别 SQL 和命令注入攻击。IBM BigFix Detect 解决方案采用高级行为分析功能来检测新威胁和回避威胁，而且能够为您提供攻击遏制和补救所需的各种工具。

意外事件响应服务

2016 年 Ponemon 进行的“数据泄露成本调研”结果显示，建立一支意外事件响应团队作为组织网络防御的一部分，能够将单条记录的数据泄露成本降低 16 美元（从 158 美元降至 142 美元）。对于意外事件而言，这种单条记录的成本降低就意味着数百万美元的成本节省。IBM X-Force Incident Response and Intelligence Services 解决方案能够帮助您高效做好准备并通过久经验证的响应战略响应网络攻击，因此是降低数据泄露总体成本的关键所在。

制造业与云

云技术正在推动着制造业的变革 [15]，因此考虑采用云技术的企业都知道，他们需要采用一种结构化的安全方法。借助 IBM Cloud Security Services 云解决方案，您可以管理数据访问、保护数据并确保可视性，而且能够提供咨询服务和托管服务。

IBM Security

增强网络安全智能功能

借助安全与威胁情报，组织可以了解他们最易遭受的攻击媒介。在了解攻击媒介之后，制造商便可领先于犯罪分子采取措施，加强内部和外部检测与保护机制。

不过，安全运营团队如何才能跟上快速剧增的威胁步伐、应对针对其组织的海量攻击？了解最新的威胁情报是风险意识的关键部分之一，但威胁数据的发展速度要远远超出人类的能力。即便是最具经验的安全专业人员，也难以完全筛选出所有的安全意外事件及可用的威胁数据。IBM QRadar® Advisor with Watson™ 是一款将认知功能与分析功能融为一体的解决方案，它能够增强安全分析师的能力，帮助他们利用来自博客、网站、研究论文等来源的无限量非结构化数据并将这些数据与相关的安全意外事件建立关联，进而识别并了解复杂威胁。

保护企业安全并降低成本与复杂性

从基础架构、数据和应用保护到云及托管安全服务，IBM Security Services 拥有丰富的专业知识，可帮助您保护关键资产。我们目前正在为一些全球最先进的网络保驾护航，并聘请了一些最优秀的人才为其服务。

IBM 提供的服务可帮助您优化安全计划，制止高级威胁，妥善保护数据并确保云安全和移动安全。Security Intelligence Operations and Consulting Services 能够参考安全领域的最佳实践评估您的安全态势与成熟度。借助 IBM X-Force Incident Response and Intelligence Services，IBM 的专家能够主动捕获并响应威胁，并在发生数据泄露之前运用最新的威胁情报做好防范。借助 IBM Managed Security Services，您能够利用业内领先的工具、安全情报和专业知识，提升您的安全态势，而且通常只需花费一点点内部安全资源。

IBM

目录

IBM Security

IBM Security 简介

IBM Security 可以提供最先进的集成式企业安全产品和服务组合。该组合由世界知名的 X-Force 研究所提供支持，可提供一流的安全智能，帮助组织全面保护其人员、基础架构、数据和应用，所提供的解决方案涵盖了身份和访问管理、数据库安全、应用开发、风险管理、终端管理、网络安全等诸多方面。IBM 作为世界上覆盖范围最广的安全研究、开发和交付企业之一，每天对 130 多个国家/地区的数十亿个安全事件进行监控，并拥有 3,500 多项安全专利。

贡献者

Michelle Alvarez - IBM Security 威胁研究员

Scott Craig - IBM Security 威胁研究员

有关更多信息

如欲了解有关 IBM Security 产品组合的更多信息，请联系您的 IBM 代表或 IBM 业务合作伙伴，或访问以下网站：

ibm.com/security

有关 IBM Security Services 的更多信息，敬请访问：ibm.com/security/services

在 Twitter 上关注 @IBMSecurity 或访问 IBM Security Intelligence 博客

[1] http://www.reuters.com/article/us-thyssenkrupp-cyber-idUSKBN13X0VW

[2] https://www.scmagazine.com/two-tech-firms-swindled-out-of-100m-were-google-and-facebook/article/653712/

[3] http://www.scmagazine.com/brunswick-corps-13000-workers-w-2-data-compromised/article/494352/

[4] https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-10908&S_KG=ov55738&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US

[5] https://www.databreaches.net/thedarkoverlord-reveals-three-more-attacks-with-more-to-be-revealed/

[6] https://www.databreaches.net/thedarkoverlord-reveals-three-more-attacks-with-more-to-be-revealed/

[7] https://securityintelligence.com/news/files-with-that-ransomware-as-a-service-lets-would-be-fraudsters-order-on-demand/

[8] https://exchange.xforce.ibmcloud.com/collection/2016-Shellshock-Attack-Campaign- ca5ef17ba943d740605597fa0fb622ad

[9] https://www.microsoft.com/en-us/cloud-platform/sql-server-2005

[10] https://capec.mitre.org/data/definitions/210.html

[11] https://capec.mitre.org/data/definitions/255.html

[12] http://searchsecurity.techtarget.com/news/450418664/Android-clickjacking-attacks-possible-from-Google-Play-apps

[13] https://capec.mitre.org/data/definitions/223.html

[14] https://capec.mitre.org/data/definitions/225.html

[15] https://www.forbes.com/sites/louiscolumbus/2013/05/06/ten-ways-cloud-computing-is-revolutionizing- manufacturing/#7d028123859c

IBM

目录

IBM Security

2017 IBM Security
75 Binney Street
Cambridge MA 02142

美国印刷
2017 年 6 月

即刻拨打咨询热线：400 810 1818 转 2395（工作日9:00-17:00），获取 IBM 专家支持
扫描二维码，关注 IBM 安全公众号，第一时间为您提供行业领先的安全解决方案

IBM

SEL03133-ZHCN-00