**IBM Security 系统** 2015 年 6 月

**IBM X-Force 威胁情报季度报告 - 2015 年第 2 季度**

不管是无心之过还是蓄意而为，内部威胁都有可能会对企业最具价值的资产造成巨大的破坏。 探索方法，对抗内部威胁。



目录

**2** 总体概述

**3** 内部威胁击碎信任链

**6** 内部威胁和不断发展的垃圾电子邮件威胁

**10** 每一次泄露都需要行动计划

**15** 身份管理有助于控制风险

**18** 关于 X-Force

**19** 作者名单

**19** 更多信息

总体概述

在本年度的第一份 IBM® X-Force® 季度报告中，我们综述了 2014 年发生的安全事件，其中表述了各产业和许多基础架构遭受了多么巨大的损害，以及改良后的攻击技术是如何改变着我们看待安全的方式。

虽然各种高级威胁和百万数据泄露事件依然占据着各大新闻头条，但是在第二季度报告中，我们将重点关注内部威胁，并探究这种内部威胁一直以来暗中为害却常常被人所忽略的原因。

根据最新的 [IBM Security 服务 2015 年网络安全情报索引](http://www-935.ibm.com/services/us/en/it-services/security-services/index.html?lnk=sec_home)显示，内部威胁在众多攻击类型当中依然高居榜首。 虽然记录显示，2014 年有 45% 的攻击事件应由外部人员负责，但仍有 55% 的攻击事件系能够访问组织系统的内部人员所为。1

在这份报告中，我们来看看这种威胁的发展过程以及公司如何减轻其所带来的影响。 “内部威胁”这个词有很多含义。从恶意员工的角度讲，他们是蓄意破坏；而对于用户来说，他们可能是无意间单击了可疑电子邮件上的附件，从而在不知觉的情况下将他们的系统 — 甚至可能是企业网络 — 暴露给恶意软件。 如今，大部分垃圾电子邮件都是为获取利益而制作的，制作者可能会将任何一种恶意软件附加到该垃圾电子邮件上。 从出于犯罪意图到为了获取经济利益，任何具有明确动机的对手都可能会雇佣垃圾电子邮件制作者精心营造一个有针对性的活动，来诱骗用户打开附件或单击链接，从而利用勒索软件或恶意软件侵染企业网络。

我们也会特别关注“准公司内部人员”，他们可能是受信任的第三方承包商。 这些人员包括电工、建筑工人、电话维修人员或者其他可进入公司内部或可访问网络的维修人员。 在美国的塔吉特 (Target) 零售百货数据泄露事件中，正是由于滥用了这种第三方访问权限，使得攻击者有机会常常盗取凭据并得以访问网络。

了解如何保护有价值的数据和资源免遭损害是大多数组织考虑的头等大事，我们会协助解释一些常见的最佳做法和建议，以启迪读者思考他们可以怎样来对抗这种风险。

在分析过程中，我们将会演示安全情报（特别是取证）如何帮助检测内部威胁并更好地分析系统和网络的当前状况。

在过去的一整年里，我们已经知道当公司逐渐了解到电脑、网络和物理安全处于一种多么危急的状况时，做好准备对于公司而言是多么重要。 通过评估受损网络可能存在的风险（无论是来自网络内部还是外部），公司就会知道未来当损害真正显现时应如何应对。

内部威胁击碎信任链

你知道谁正在访问你的资源吗？ 探索在当今不断变化的商业环境中如何保护自己的重要资产不受侵害。

**对**于大部分企业来说，“内部威胁”曾经意味着心怀不满或粗心大意的员工对公司的物理或电子资产造成的伤害。 随着过去十年间企业和政府所资助的间谍活动不断升级，现在要保护您的所有资产的安全，还需要考虑到各种各样其他情况。

评估内部威胁的风险时，许多公司会着重关注“受信任”的员工，特别是那些特权级别较高的员工。 当这些员工访问和处理重要的商业和货币资产时，公司依赖于他们会遵守严格的隐私权需求。 这些特权用户应该严格遵守策略，而不会擅自利用其强大的访问能力。 因此，公司应巧妙平衡在高利害关系的商业环境中给予用户的信任和访问特权之间的关系。

组织希望信任员工，但他们也必须核实其最具价值的资产将会发生的活动。这些最具价值的资产有如“皇冠上的珍珠”，包括知识产权、金融数据、产品设计以及其他对于商业成功至关重要的信息。 正因为这些数据价值巨大，所以往往成为内部威胁的目标。

在如今的就业市场，劳动者经常每隔几年就更换工作，力图实现自我成功，不会全心奉献于任何一个组织。 通常，当这些员工进入到对手公司后，他们在原公司仍然会有一些能够访问资源的朋友。 出于对原公司的不满情绪或寻求某种捷径等种种可能性，导致近来的安全泄露事件屡屡成为新闻头条。 离职员工在离开公司前可能已建好了“后门”，一旦她/他进入了新公司就可能会启用这个后门，从外部访问隐藏的账户或敏感数据。 这并不是突然萌生的猜想，而是几乎每天都会有公司报告的活动。 要帮助您时刻保持警觉性，比较有用的方式是设置一种重复处理程序来复查访问日志和网络活动，以查找这些后门或

其他任何看起来很奇怪或不同寻常的行为。 也可以使用自动监视服务，但通常这会导致如何平衡风险与公司成本的问题。

保护客户数据安全没有捷径，不应该是轻轻松松就能完成的。 最近的内部威胁甚至已经震惊了一些从事客户隐私信息数据库维护的重要供应商，这些供应商已经建立了完备的内部流程。 例如，去年第三方供应商内部的恶意员工曾伺机盗取了全球电信公司的客户数据（包括出生日期和美国社会保险号）并使用这些信息解锁了移动电话在黑市上转售。2

必须有目的有意识地监视存放最重要资产的电脑网络，以确保这些资产不会通过网络连接、电子邮件、USB 设备或其他任何方式泄露。 公司不仅应该设置限制，规定只有需要访问隐私数据（包括客户数据）的员工才能具有特别访问权，而且应该对异常的员工活动进行监视。

另一方面，如果客户遇到供应商仅仅只要求您提供隐私细节，也也应该警惕。 一旦公司拥有了客户的敏感隐私数据，即表示该客户接受该公司的数据保护策略和做法，而对于客户而言，评估或理解这些策略和做法可能是非常困难的。

许多组织选择放弃安全升级，直到发生了严重的事故，他们才会花钱补上某些安全措施，或者制定一些早在多年前就应该到位的策略，但通常为时已晚。 对于许多组织来说，维护技术资产、数据或物理资源的安全往往不受重视，因为维护安全所耗费的成本常常会对现金流带来负面的影响。

从物理安全到社交工程，威胁无处不在

许多人认为与 IT 相关的安全止于公司的电脑网络以及各种连接设备或技术。 但是，数字威胁并不始终限于 IT。 在许多情况下，数字网络也允许访问公司的物理安全系统。

因此，数字威胁可能会影响警报系统，特别是那些允许通过 Internet 远程监视的系统。 连接 Internet 的电话系统也会受到影响，这些系统在组织内部或外部都可能遭受损害。 几年之前，研究人员演示了从世界的任意一个地方远程启动电话的麦克风进行窃听有多么容易。3如果“网际网络语音协议 (VoIP)”电话配有 Webcam，那么任何一个不需要具有太高智商的人都可以启动该电话。3

这项研究表明，评估电脑网络的威胁时，对整个系统进行全面细致的评估是非常重要的。 例如，有一种较低级别的针对公司复印机和传真机的威胁。 现在，这些机器大部分（即使不是全部）都配备有某种类型的内存或硬盘驱动器，并且通常都会连接到内部网络。 任何一个具有适当技术知识的人（例如，维修技术人员）都可以快速访问这些存储设备，并盗取重要数据。 而且，通过网络也可以访问此类存储设备。

事实上，有些研究人员已在从 eBay 上购买到的复印机硬盘驱动器上，以及从企业报废设备的销售人员和政府设备拍卖那里购买到的复印机硬盘驱动器上，发现敏感文档。 在这几个案例中，甚至都不需要入侵电脑，只要知道如何拔下硬盘驱动器再将它挂到电脑上就够了。 在很多情况下，硬盘驱动器设计为只能用于 Linux 或 Microsoft Windows。 更换复印机或传真机时，务必确保由本公司而不是第三方公司来保存或销毁数据。

**内部威胁的攻击媒介**

进入物理系统的数字入口点 — 攻击者可以使用警报系统、复印机和传真机以及连接 Internet 的电话系统作为入口点来访问敏感数据。

第三方承包商 — 维修工人、现场服务技术人员和保洁人员通常可以在无人陪伴的情况下进入，这使得他们有机会篡改系统，并获得记录在员工工作区的密码。

“准公司内部人员”是对企业安全的另外一种的威胁，虽然级别较低，但不应忽视。 在电子通讯出现之前很久的时间里，这种威胁一度是谍报技术的主要形式。 许多企业都有来自维修保养公司、建筑公司和保洁公司的承包商，他们可以在工作日的非工作时间或周末进入工作区。 这些人通常可以在无人陪伴的情况下进入整个企业空间，可能包括企业最高管理层办公室和董事会议室等区域。

这种由于第三方人员进入而导致损害的一个示例就是最近的塔吉特 (Target) 数据泄露事件。 在此案例中，攻击者利用从制冷和空调承包商处窃取的凭据成功盗取大约 1.1 亿人的个人和金融信息，致使 11 GB 数据受损。4 此案例表明，无论在时间还是金钱上，都必须对保护那些可进入公司网站或 Web 服务器的非“前门”入口的安全予以极大的关注。 许多公司还需要特别关注对于向经销商、承包商或合作伙伴开放的其他一些入口点的控制。

而且，在国际舞台上，由于缺乏监督而导致的安全漏洞为民族国家或其他对手在不知不觉间进行渗透和访问企业资产创造了成熟的条件。 接受过正规间谍训练的工作人员只要几分钟时间就可以在企业最高管理层的办公室或董事会议室内安装一个窃听设备。 他们所接受的“训练”可能仅仅是“将这个插入墙中或放到它前面的植物中”，或者也可能更加严格，更加复杂。

几分钟之内，一个未经授权的人就可以一边擦拭员工的桌子，一边找到某个人写在抽屉、笔记本或办公区域中其他地方的密码。 如果未经授权的人可以从企业内部某处（例如，员工工作区）访问企业网络，那么他们几乎没有任何被发现的风险，就能够造成巨大的伤害。 通过访问复印机或传真机，他们可以在几分钟之内换出或复印存储设备并下载其中的内容。 虽然上锁或者贴上防破坏保护贴也可以对机器进行保护，但这并不能完全防止这些机器受到损害。 对企业最高管理层办公室和董事会议室进行电子扫描也是一种保障。

有多种防御性级别可供公司使用，无论数据泄露是由企业或国际间谍所为，还是仅仅因为个人追逐私人利益所致，只要公司感到其数据安全存在风险，就可以采用。 例如，如果公司是租用公共楼宇，那么需要防备该楼宇所有者。 此外，还须对与公司办公场所处于同层或上下层的邻居有所了解。 了解并保护存储数据的物理位置非常重要。 历史证明，就近攻击资产非常方便。

最后的想法与建议

在当今的商业环境中，公司重要资产的防盗转工作愈发具有挑战性，因为内部和外部对手有意愿、有信息、有资源而且有耐心寻找机会，未经授权进入。 企业应拨出预算用于安保措施，以协助防止盗窃事件的发生。 这些安保措施包括针对物理安全和技术部署适当的控制，以及全面了解为组织工作或代表组织的员工或承包商。

对于那些一直致力于保护其最具价值的资产免遭数字敌手的侵害，却忽视了内部有机会访问这些最具价值资产的员工或承包商可能造成的威胁的组织，第三方评估可能会有所启发。 有一些具有专业知识和技能的人可以就他们能够轻易观察到的弱点提供意见和建议，从而为您提供帮助，但他们的意见和建议可能会与您的企业文化相冲突。 在这些专家当中，有很多人具有多年在军队或联邦政府的供职的经历，他们在多年的谍报与反谍报活动中积累了丰富的技能。

简单的解决方案可能是，当有外部人员可以进入具有敏感数据或设备的区域时，由公司人员进行陪同。 这看似一种负担或对于公司资产的浪费，但从长期来看，相对于因最具价值的资产遭到入侵或窃取所致的数百万美元的损失，这是很“便宜”的。 在某些政府办公室，任何进入办公空间的承包商都必须有人陪同，或者提交背景调查。

当需要雇佣或聘任最佳员工担任敏感职务，或者与某人签约以允许其访问基本的公司数据时，在雇佣过程中调查该人员的背景永远都是好办法。 大部分公司已经针对某些职位进行入职前的毒品检测和犯罪记录调查。

内部威胁和不断发展的垃圾电子邮件威胁

通过垃圾电子邮件分发恶意软件呈上升趋势。 了解如何保护您的公司并使用户保持警惕性。

**威**胁可能源自于组织外部，也可能来自于未经授权或心怀不满的内部人员。但是，任何内部人员，即使是怀有良好意愿的人员也可能由于

单击了网络钓鱼电子邮件中发送的恶意链接而无意间帮了攻击者的忙。 要防止此类事件发生，组织的安全小组需要识别通过垃圾电子邮件分发恶意软件的危险，并采取措施封锁它。 每位用户都应该常备不懈，时刻警觉到即使是最单纯的一个动作也可能会为攻击敞开大门。

信息安全专家有时更多地是将花园变异垃圾电子邮件视为一种滋扰而非威胁。 毕竟，诸如网络钓鱼或鱼叉式网络钓鱼攻击、恶意软件或“分布式拒绝服务 (DDoS)”等威胁已将他们的时间占满。 不过，最近的 IBM X-Force Advanced Research 分析指出，来自于垃圾电子邮件的威胁日益增长，这可能需要大家更加认真地对待。

要调查最近的垃圾电子邮件活动，了解这些垃圾电子邮件是从哪些国家发出来的是一个很好的切入点。 图 1 显示最近两年各国发出垃圾电子邮件的趋势。

在此图表中，显示了数年内逐年的起伏波动。 一些关键点包括：

* 2015 年第一季度，美国发送了最多的垃圾电子邮件，占比超过垃圾电子邮件总量的 8%，这表明分发垃圾电子邮件的力量有多么广大。
* 越南在去年年底曾在此数据上称霸，但现在只屈居亚军。
* 在过去的两年时间里，西班牙曾数次占据发送垃圾电子邮件数量之冠，但如今也只屈居第三位。
* 在最近一个季度，所有其他参与调查的国家的垃圾电子邮件发送量占全球垃圾电子邮件发送量的 6.1% 到 1.1% 之间，并且在过去的两年里有数次起伏波动。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 垃圾电子邮件发送量最高的国家  从 2013 年 1 季度到 2015 年 1 季度 | | | | | | | | | | | | | |
| 14% | 西班牙占据垃圾电子邮件发出地的榜首 | | | | | | | | | | | | |
| 12% |
| 10% |
| 8% |
| 6% |
| 4% |
| 2%  0% |
|  | 2013 年 1 季度 | 2013 年 2 季度 | | 2013 年 3 季度 | 2013 年 4 季度 | | 2014 年 1 季度 | | 2014 年 2 季度 | 2014 年 3 季度 | | 2014 年 4 季度 | 2015 年 1 季度 |
|  | 阿根廷 (AR)  意大利 (IT) | | 中国 (CN)  俄罗斯 (RU) | | | 德国 (DE)  台湾 (TW) | | 西班牙 (ES)  美国 (US) | | | 印度 (IN)  越南 (VN) | |  |
|  |  |

图 1 2013 年 1 季度到 2015 年 1 季度垃圾电子邮件发送量最高的国家

看着这些数据，有人可能会觉得没有什么新鲜的。

查看过去两年的垃圾电子邮件数量（如图 2 所示）时，也可能会有相同的看法。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 垃圾电子邮件数量  2013 年 1 月到 2015 年 3 月 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 300% | 与 2013 年早期的数量差不多  自从 2010 年 8 月以来的最高数量 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 250% |
| 200% |
| 150% |
| 100% |
| 50% |
| 0% |
|  | 2013 年 1 月 | 2013 年 2 月 | 2013 年 3 月 | 2013 年 4 月 | 2013 年 5 月 | 2013 年 6 月 | 2013 年 7 月 | 2013 年 8 月 | 2013 年 9 月 | 2013 年 10 月 | 2013 年 11 月 | 2013 年 12 月 | 2014 年 1 月 | 2014 年 2 月 | 2014 年 3 月 | 2014 年 4 月 | 2014 年 5 月 | 2014 年 6 月 | 2014 年 7 月 | 2014 年 8 月 | 2014 年 9 月 | 2014 年 10 月 | 2014 年 11 月 | 2014 年 12 月 | 2015 年 1 月 | 2015 年 2 月 | 2015 年 3 月 |

图 2. 2013 年 1 月到 2015 年 3 月的垃圾电子邮件数量

虽然我们已经看到了过去两年间的垃圾电子邮件总量的主要波动起伏状况，但是当前的数量与两年前的数量相当。

不过，我们并不应因此得出结论说，垃圾电子邮件领域并未发生任何变化。 图 3. 传输恶意附件的垃圾电子邮件百分比显示了主要变化。

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 带有恶意 ZIP/RAR 附件的垃圾电子邮件百分比  2013 年 1 月到 2015 年 3 月 | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9% | 从 10 月到 2 月，大约有 4% 的垃圾电子邮件传输了恶意附件  自从 2012 年 11 月以来观察到的最高值 | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8% |
| 7% |
| 6% |
| 5% |
| 4% |
| 3% |
| 2% |
| 1% |
| 0% |
|  | 2013 年 1 月 | 2013 年 2 月 | 2013 年 3 月 | 2013 年 4 月 | 2013 年 5 月 | 2013 年 6 月 | 2013 年 7 月 | 2013 年 8 月 | 2013 年 9 月 | 2013 年 10 月 | 2013 年 11 月 | 2013 年 12 月 | 2014 年 1 月 | 2014 年 2 月 | 2014 年 3 月 | 2014 年 4 月 | 2014 年 5 月 | 2014 年 6 月 | 2014 年 7 月 | 2014 年 8 月 | 2014 年 9 月 | 2014 年 10 月 | 2014 年 11 月 | 2014 年 12 月 | 2015 年 1 月 | 2015 年 2 月 | 2015 年 3 月 |

图 3 2013 年 1 月到 2015 年 3 月期间附带恶意 ZIP/RAR 附件的垃圾电子邮件百分比

截止到 2013 年夏天，附带恶意软件的垃圾电子邮件百分比仅超过 1%。 之后，在该年秋天，出现一次较大幅度的增长。 2015 年前几个月期间，带有恶意附件的垃圾电子邮件百分比已达大约 4%。 因此，虽然过去两年间垃圾电子邮件的总量未发生变化，但是较之以往，垃圾电子邮件制作者现在正在更多地利用这个渠道来散布恶意软件。

此当前趋势符合我们在[“IBM X-Force 威胁情报季度报告 – 2015 年第一季度”报告](http://www-03.ibm.com/security/xforce/downloads.html)中报告的趋势。 当时，我们将该恶意软件的级别定为最普通的攻击类型之一，带有恶意附件的垃圾电子邮件提供了将恶意软件带入公司网络并放到用户电脑上的途径。

任何类型的恶意软件都可能附加到垃圾电子邮件上，因为只要在垃圾电子邮件中加入链接，就可以将其发送到任何地方。 许多垃圾电子邮件制作者将此经营为一项盈利性的商业活动，在这里，是由买家而不是垃圾电子邮件系统操作人员来决定邮件所附带的内容。 任何对手、出于任何目的（从出于犯罪意图到为了获取经济利益）都可以雇佣垃圾电子邮件制作公司。 就如同轻易就能够对个人用户带来不良后果一样，利用勒索软件入侵您的企业网络可以轻易对您的业务带来巨大的风险。 此外，对您的知识产权和商业秘密更感兴趣的对手可以使用垃圾电子邮件，通过键盘记录和密码窃取工具渗透到您的网络。

通过这些观察，我们可以得到几个结论。 最重要的是，垃圾电子邮件日益变得更加危险。 过去，垃圾电子邮件的行为主要是说服受害者购买某些东西或陷入某个骗局。 随着时间的推移，垃圾电子邮件逐渐开始尝试利用恶意软件侵染机器。 这种趋势推高了可靠的垃圾电子邮件过滤在网络安全中的优先级。 由于没有任何技术可以确保防范效果完美无缺，我们必须教育用户学会态度更加坚定，不要轻易被说服。

建议

以下是给网络管理员的一些建议，以协助他们提防恶意垃圾电子邮件附件。

* 时刻保持垃圾电子邮件和病毒过滤器处于最新状态。
* 封锁可执行的附件。 在常规的业务环境中，发送可执行附件是不正常的。 大多数垃圾电子邮件过滤器都可以配置为封锁可执行文件，即使这些文件是放在压缩附件中。
* 使用邮件客户端软件来禁止自动渲染附件和图片以及预先载入链接，并随后将其禁用。

提升用户的防御姿态呈现出更加需要技巧的问题。 需要由用户来警惕危险，并随时随地应用常识。 打开电子邮件并单击链接或打开其中包含的附件之前，用户应先问几个简单的问题：

* 我认识发件人吗？
* 我预计应该收到这封电子邮件和附件吗？
* 附件有必要压缩吗？其格式对于这种类型的邮件和附件类型来说适宜吗？
* 压缩文件中是哪种文件类型？ 如果是可执行文件、屏幕保护程序或者我不认识的文件类型，我不应该打开它！

垃圾电子邮件制作者通常会使其制作的电子邮件看起来非常像来自网上商店、银行或金融机构、或者网络内部系统（例如，传真机和复印机）的标准邮件。 用户对于这些电子邮件也必须持怀疑的态度。

每一次泄露都需要行动计划

了解取证分析如何提供您所需的洞察力，来理解您的网络中发生了什么，以及需要哪些步骤来阻止威胁。

**保**护网络免遭潜在的损害近似于飞机驾驶员 - 数月的百无聊赖，一时的惊心动魄。 就像训练飞机驾驶员

有条不紊地应对任何飞机故障一样，安全专家也需要接受训练并拥有工具，以便能够有条不紊地应对其网络资产可能遭受的任何损害。

安全系统的定义是，破坏系统所需的付出远超可能获得的利益。 不过，付出和利益的目标是不断变化的。 当对手们互相交流其黑客工具，共享其技术并合作攻击明确的目标时，破坏组织所需的付出就会降低。 所获得的回报通常也会大到足以鼓舞黑客军团根据最新发布的漏洞开发复杂的软件来测试并渗透网络。 当一个新的漏洞被公布，而后这些专门的黑暗应用程序测试并探查服务时，目标公司的安全专家可能会看到他们的网络“亮了起来”。

因此，重点不是您的网络是否将要遭受损害，而是您是否已做好准备，以及对于攻击，您将如何予以回击。 想象一下，如果一个驾驶员没有接受过故障训练，会是怎样的情形？ 不可能会是美好的结果。 现在，想象一下，一个没有取证能力的网络会怎样？ 前景也不会乐观。

例如，如今的消费者经常会收到其医疗、银行和电子商务提供商发来的邮件，告知其自身网络已遭受损害，但是，这些公司无法对这些损害进行清晰的描述。 在很多情况下，唯一的解决方法就是，由客户来修改其信用卡和登录身份，并重设密码。 然而，更加严重的后果是，用户根本无法找回其社会保险号码、地址、电话号码以及其他个人身份识别。

那是因为，虽然丢失一份个人身份识别可能并不是严重的问题，但是，如果网络犯罪分子获得了某个人的所有个人身份中包含的关系或关联，那么他们就获得了通过电子手段进行金融盗窃和欺诈所需的大约 95% 的数据，无论受害者是否已修改其信用卡号码，结果都一样。 而且，如果提供商无法清楚地识别出该损害是如何实施和操控的，他们就不可能确保此类损害不会再次发生。

具备精确识别损害的能力是任何一家保有利于电子犯罪的信息的公司的基本原则。

网络和资产取证

取证是清晰地重建并描述出系统中的任何损害的能力。 基本功能包括数据包捕获、搜索、过滤重建和微检查。

**数据包捕获**

“捕获”是指收集和存储网络上发生的每一次交易的能力。 它提供了交易的可见性以便进行取证，同时，它也需要巨大的存储能力。 例如，要存储以 60% 容量运行的 10 GB 链接的网络流量每天的存储量大约为 7 TB。 一个容量为 56 TB 的典型 2 机架单位 (2U) 捕获装置可以存储 8 天的网络历史数据。 此时间段称为可见性的取证期间。 期间越长，可用于取证分析的可见性就越多。

由于许多损害发生的时间段都更长，因此，以最低的成本提供最长的期间显得格外重要。 启用数据包捕获的最大费用是存储成本，因此，以较低的价格获得存储空间来提供更长的可见性期间至关重要。 主要存储供应商在其产品中实施压缩技术，从而使系统容量提升高达四倍。 图 4 显示在使用和不使用压缩技术的情况下，捕获 10 GB 网络所需的成本。 在此情形中，使用压缩技术将成本降低了四倍，这样，以未压缩存储空间的成本可存储几乎 45 天以上的数据包捕获。

**搜索**

取证调查通常是指搜索未知的内容。 在这方面，搜索引擎技术可通过提供以下支持来提供帮助：

* 熟悉易用的搜索界面
* 所有取证数据的 100% 瞬时可见性

例如，任何人在 Internet 上搜索包含 [support@corporatebank.syzexperts.com 的文档时，都会马上收到结果。](mailto:support@corporatebank.syzexperts.com) 将搜索引擎技术应用于取证时，其对于捕获的网络流量也会提供同样的功能。 上面的示例电子邮件地址是网络钓鱼尝试中可能使用的一种典型示例，其中的公司名牌 (corporatebank) 会内嵌在攻击者的域中 (syzexperts.com)。 设置了适当索引的搜索引擎技术会立即发现使用该地址的网络交易。

绝对可见性要求对捕获数据包的全部内容设置索引。 在设置索引过程中，搜索引擎会将数据分类到启用高保真查询的各个字段中。 例如，网络流量按照 Web 域、电子邮件地址、URL、HTTP 错误码以及数以百计的其他字段来设置索引，以启用特定查询。 来看看下面的查询：

IPAddress:192.72.68.121 AND Port:880 AND URL:\*$^% AND HTTPError:404

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 数据包捕获  成本与可见性期间 | | | | | | | | | | | |
| $1,000 |  | | | | | | | | | | |
| $800 |
| $600 |
| $400 |
| $200 |
| $0 |
|  | 0 天 | 10 天 | 20 天 | 30 天 | 40 天 | 50 天 | 60 天 | 70 天 | 80 天 | 90 天 | 100 天 |

未压缩 已压缩

图 4 数据包捕获、成本与可见性期间

此查询使取证调查人员能够搜索通过使用奇怪的字符来扰乱“具象状态传输 (REST)”界面以混淆 HTTP 应用程序服务的任何尝试。 取证调查人员可能想要优化对于网络钓鱼尝试的搜索。

From: \*syzexperts\* AND password

此搜索将找到电子邮件名称中包含 syzexperts 且邮件正文内容中包含文本密码的所有电子邮件流量。

**过滤**

搜索未知内容时，必须确定哪些内容重要，哪些内容不重要。 取证能力应该包括轻松过滤和显示数据的能力，它应该能够区分重要与琐碎的内容。 例如，研究人员可能会发现，网络中的某些域出现了奇怪的行为。 只要搜索 DNS 流量并显示端点关系即可快速发现报告中尚未有的“异常值”。 例如，图 1 显示了特定查询的所有 DNS 流量。 这种具象化的显示清晰地呈现了常规操作之外解析的两个异常值域。 此可视化描述为调查人员进一步检查这些异常值提供了清晰的开始点，而这些在标准报告中是无法获得的。

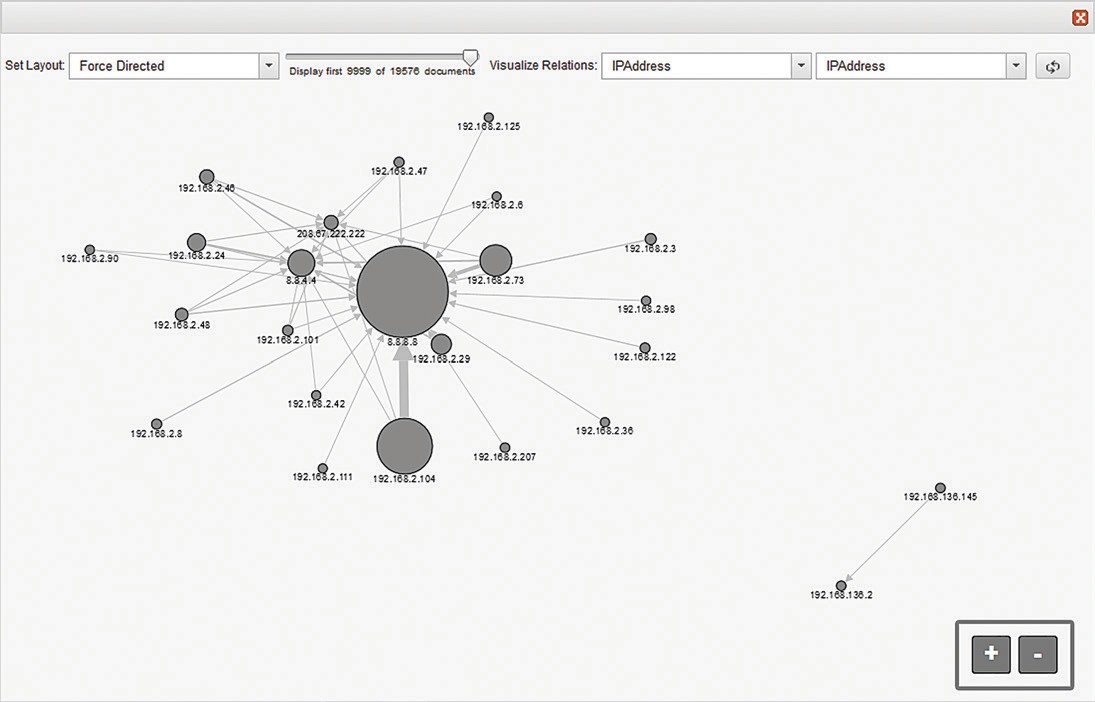


图 1. DNS 网络实体关系

**重建**

通过重建，组织可以查看以适合于人类使用的格式记录的网络交易。 存储系统中包含从网络捕获的原始的、难以理解的流量数据块。 这些原始数据必须经过仔细研究和分析后，才能用于重建。 重建示例包括显示对手访问过的网页，涉及到的完整的电子邮件（线程）、攻击中被盗窃的文件，或者，甚至还包括整个 IM 对话。

在重建过程中，名为检查器的软件模块会将网络数据细分为用于搜索和重建的中间形式。 检查器会通过电子流中的位模式来识别网络流量。 基于数据模式而不是端口号来识别流量非常重要，因为攻击者可能会尽力伪装协议。 检查器是由工程人员编写的，他们会分析那些协议和服务，来提取关键字段元数据。 这些元数据以一种结构化的格式放入搜索引擎，这种格式能够确保详细地重构网络事件。 评估一种取证解决方案的能力时，非常重要的一点是了解识别协议与检查协议之间的差异。 许多供应商声称拥有数千种协议标识符。 标识符仅会标记所使用的协议，检查器会对协议进行细分以用于搜索和重建。

以下是不同类型的重建：

* 网页
* 聊天
* 社交网络
* Webmail
* 博客创建
* 文件传输
* 文件附件
* 文件元数据（地理位置、上次修改时间以及其他类似的属性）
* 文件流（附带的可执行文件、JavaScript、宏、重定向）

**微检查**

搜索和重建会将感兴趣的网络交易从可能数万亿的流优化为可管理的集。 微检查会通过识别可疑内容或数据来细分最后的分析（例如，对内嵌文件、文件平均信息量、混淆文件、文件沙盒和文件流、宏、可执行文件等进行报告），精准确认战略取证信息。 首要检查环境包括自动提取详细文件信息的能力。 在文件中内嵌信息和文件以及混淆文件类型是攻击者们使用的重要方法。

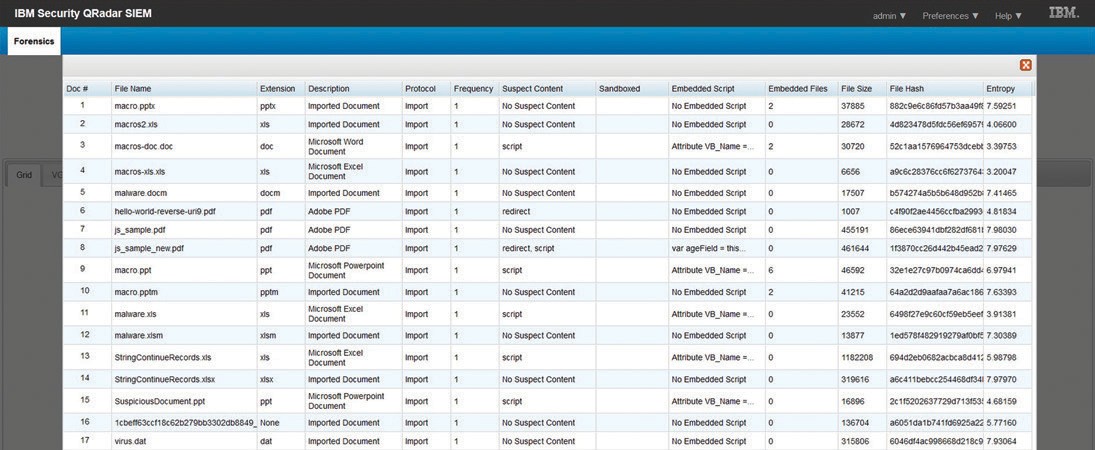


图 2. 微检查网络事件中的所有文件

取证系统会使用各种方法来检测内嵌文件，包括“幻数”和统计分析。 幻数是文件标识属性，在一个文件中检测到多个幻数是提醒调查人员存在可疑的内容。 统计分析用于判定数据流或文件内容的“常态”，并有可能会检测到数据注入到文件或数据流中的时间。

其他文件微检查技术包括文件反混淆技术，此技术会将文件扩展名与 MIME 和内容类型进行比较。 例如，攻击者常常会将可执行文件伪装成图片文件。 将文件流附加到文档上也是攻击者常用的方法，用来执行该文件中内嵌的恶意软件（宏、JavaScript、可执行文件、URL 重定向等）。

沙盒为取证分析提供了用以确定攻击感染主机方式的终极的工具。 图 2 显示了对于在优化的网络流搜索中找到的文件执行微检查的能力。

摘要

重建网络损害期间发生的活动的能力对于保护网络安全和阻止进一步伤害来说非常重要。 在许多情况下，很难准确检测到损害，首要取证环境的搜索功能是它所提供的基本功能。 通过捕获并为所有数据设置索引来实现网络流量 100% 可见性的能力，使得调查过程非常清晰可视。 提供可见性、衍生情报以及微检查能力的增补工具会极大地降低评估损害的时间，并且可以准确地描述出破坏的范围以及防止进一步破坏所需的安全改进和加强。

身份管理有助于控制风险

您的所有员工（尤其是特权用户）都可能会威胁到您的系统。 了解正确的工具如何协助管理这些风险。

**事**实上，对于您的业务资源（包括最具价值的业务数据）的威胁可能来自于组织的任何地方和任何人。 因此，您需要

一整套工具来控制风险。 这些工具必须能够到达企业的每个角落，能够帮助您洞察所发生的每个行动，并且能够帮助您管理访问您的环境的每一个人。

您的员工可能是您最脆弱的链条

如今，在许多组织中，最严重的安全威胁不是外部攻击，而是内部人员，他们可能会损害或泄露敏感数据。 企业计算的现代化趋势（社交媒体的兴起、云、移动和大数据时代）使得来自员工、承包商、合作伙伴以及拥有受信任访问权的其他人员的威胁变得更加难于识别，同时为内部人员提供了更多传递受保护信息的途径，而且更加不易被发现。

可能造成内部威胁的违法者范围广泛，他们将组织及其资产置于风险之中。 虽然恶意员工是明显的威胁来源，但无意间暴露系统而遭受攻击或者因失误而为恶意软件敞开大门的用户也同样是威胁来源。 即使公司拥有强有力的安全做法，在面对能够帮助网络犯罪分子盗取访问凭据的社交工程时，也仍然非常脆弱。 例如，在一个案例中，攻击者向可信任的员工发送附带了恶意软件的电子邮件，以获取对该供应商客户数据的访问权。5

明确教育员工警惕可疑的通讯和潜在的风险非常重要。 但是，这些努力还必须有其他更加强大的自动化威胁保护工具和全面的安全策略作为支撑。

使用 IAM 解决方案减轻内部风险

“身份和访问管理 (IAM)”解决方案在对抗内部威胁，协助减轻安全泄露或因用户拥有过时或不适当的访问权限级别而导致的违规所带来的威胁方面扮演着重要的角色。 事实上，如果用户的配置文件所授予的资源访问权没有反映当前需要和实际的使用模式，那么会发生内部威胁活动的可能性要高得多得多。 实施攻击的内部人员也可能会利用控制不力的管理特权来扩大攻击或更改系统以进行窃听。 对于用户访问特权监控不力，再加上缺乏对于误用或滥用这些特权的监察，常常在帮助这些内部攻击顺利实现上起了很大的作用。 因此，必须时刻确保访问特权与已确立的安全策略保持一致，并且审核和报告工具也应到位，以监视用户的行为并强制执行这些策略。

面对内部威胁时，保护有价值的数据和资源不仅仅是要求每个用户有一个简单的用户 ID 和密码。 你需要强有力的身份验证，这依赖于健全的身份验证策略。 这不仅有助于防止坏人从外部攻击组织，而且有助于减少疏忽大意的内部人员无意间泄露数据的机会。 还有助于防止恶意的内部人员利用疏于管理的过期或无主账户攻击您有价值的资源。

组织还应使用身份管控解决方案来协助根据角色和访问需求对用户进行分类，并设置和强制执行基于角色的策略来自动执行用户生命周期和密码管理。 仅仅允许或拒绝对应用程序的访问是不够的，您还必须知道请求访问的人员和原因，以及当他们获得访问权后，会利用这些访问权做些什么。 IAM 解决方案还应执行监视和强制功能，以协助监察身份策略违规和身份滥用，这些都可能暗示存在内部威胁。

特权用户通常是最大的威胁

在当今的 IT 基础架构中，数据集中处理、云计算、虚拟化以及外包的趋势产生了更多的特权 ID。 这为集中管理并保护特权 ID 的安全，以及注意为谁授予特权 ID 状态创造了更大的需求。 这些特权用户巨大的访问权使他们获得了控制和利用组织数据、应用程序和端点的特殊能力。 如果特权用户 ID 没有得到适当的管理，他们不仅会增加数据失窃的风险，而且可能会导致责任关系和合规性的问题。 同时，对于其他组的内部访问控制虽然特权级别较低，但仍然存在很高的风险，也不应忽视。 系统管理员和其他 IT 员工可能具备发动内部攻击的技能，也不应被忽略。 如图 5 所示，最近的 IBM 研究中所调查的决策制定者已经认识到管理员和特权用户所带来的安全威胁。

幸运的是，组织可以采取许多方法来减轻内部威胁。 更加严格的策略控制以及提升对用户的教育是很好的开端。 这意味着确保整个组织的员工都意识到他们对于特殊活动的职责和责任关系，以及如何避免攻击和不适当的访问。 公司还需要确保员工了解最新的法规和合规性要求。

这些措施需要有效的安全工具来支持。 能够监视行为并提供异常检测的安全情报解决方案是非常宝贵的，监控“超级用户”访问权的特权身份管理 (PIM) 解决方案也同样非常重要。 身份管控工具可以协助确保用户的访问权利与其工作责任相对应。 如果将情报与管控解决方案集成到一起，就可以有力地协助对抗恶意的内部人员。

IBM 商业价值研究院的调查中报告的最主要的安全威胁

|  |  |
| --- | --- |
| 劣迹管理员/特权内部人员造成的损害 | 48% |
| 来自社交媒体活动的威胁 | 41% |
| 通过使用供应链中的产品（固件、中间软件、工具包等）而插入的后门或隐藏功能 | 38% |
| 产品中插入恶意软件或本身潜在的漏洞 | 38% |
| 对于企业的高级的顽固的威胁 | 36% |
| 由于员工的移动设备和“自携设备 (BYOD)”而导致的威胁 | 36% |
| 由于设备丢失或被盗而导致的威胁 | 35% |
| 云计算特定的威胁 | 30% |

图 5 IBM 商业价值研究院的调查中报告的最主要的安全威胁

来源： IBM 商业价值研究院，IT 基础架构研究；Q7： 你有多担忧下面的安全威胁？

**使运营智能成为您的秘密武器**

要有效对抗内部威胁，必须建立和维护访问权控制，并监视那些通常可以自由访问组织最敏感数据的高级经理和行政人员，这非常重要。 如果没有适当的监督，那么，几个月前离开组织的高级人员，甚至已潜入您的系统的攻击者都可以使用某个行政人员的特别访问权访问您的服务器、装置、网络和数据。 如果能够更好地监督这些用户及其行为，那么当保密信息受到不适当的访问、分发和下载时，就会升起红色标帜。

要协助确保用户责任关系并减轻内部威胁，组织应该考虑在整个企业内实施由分析和安全情报支持的 IAM 方法。 利用这些方法，组织可以快速准确地识别用户行为中的异常之处，了解用户角色和组成员身份，防止内部欺诈，以及展示是否符合快速发展的安全规范。

集成身份情报系统也可以监视用户活动，这是积极防御内部威胁的一个至关重要的组成部分。 例如，搭配使用安全情报分析和报告工具，可以为审核用户活动和发掘可疑行为提供重要的能力。 用户活动监视解决方案基于安全情报来提供对于用户活动及其影响的全面可见性。

安全情报也可协助检测较长一段时间内发生的内部威胁。 有些解决方案专门针对特定的事件、资产或交易类型，以便存储和分析的数据量更少，更加易于管理。 这使得识别来自内部的“低而慢”的攻击成为可能。 最重要的是，有了安全情报，企业不必再回答“发生了什么？”这样的问题，而是预告“要发生什么？”，从而协助组织防止可能会发生的泄露。

建议

那么，什么才是协助您更好地减轻内部威胁并强化合规性的最佳做法呢？

**特权 ID 不断增加，因此，需要控制相关风险。** 组织常常会将特定的管理任务委派给一群员工或承包商，他们的成员身份会经常发生变化。 此外，应用程序所有者和开发人员等员工可能需要偶尔或者一次性的特别访问权，来访问特定的资源以便执行维护任务。 这两种做法都可能会导致组织内提供的 ID 数量激增。 但是，虽然让多个特权用户针对每个资源共享一个或多个普通用户 ID 可以快速控制 ID 数量的增长，但这并不是好办法。 这种做法虽然可以规避因用户的来去而不断添加和删除账户的需求，但是这也破坏了用户的责任关系。 除了破坏用户的责任关系，还可能会干扰合规性。 首选解决方案是部署身份管理系统，该系统不仅可以为 IT 员工共享特权 ID 提供安全便利的方法，而且还可以审核追踪每个用户的行为。

**授予用户适当的权利并随时更新。** 用户权利应根据变化进行更新，特别是当员工角色发生变化或离开组织时。 相对而言比较简单、每个组织都可以采用的最佳做法是，根据用户所需的最低访问特权对用户进行授权，然后定期对用户权利进行审核。 由于权利的增长与潜在的伤害是成正比的，所以应将特权账户的数量控制在最小范围。 授予特权 ID 权利时应仔细审查，并且只能授予那些真正需要特别访问权的人和具有必要的凭据和证明的人。

**管理并监视用户以确保安全和合规性。** 用户账户一旦建立，组织就应该小心监视并审核与该 ID 相关的活动，以便突出显示该账户特权有无异常之处或误用行为。 通过将用户和应用程序的监视活动与应用程序层网络可见性结合起来，组织可以更好地检测出有意背离正常活动的行为，从而协助阻止攻击彻底完成。

关于 X-Force

高级威胁无处不在。 借助 IBM 专家的洞察力协助您将风险最小化。

IBM X-Force 研究和开发小组研究和监视最新的威胁趋势，包括漏洞、攻击、活动的攻击、病毒和其他恶意软件、垃圾电子邮件、网络钓鱼以及恶意的 Web 内容。 除了建议客户和公众注意新出现的和严重的威胁之外，IBM X-Force 还会交付安全内容，来协助保护 IBM 客户远离这些威胁。

IBM Security 合作

IBM Security 代表若干个品牌，共同提供广泛的安全能力：

* IBM X-Force 研究和开发小组会发现、分析、监视并记录各种各样的电脑安全威胁、漏洞以及攻击者的最新的趋势和使用的最新方法。 IBM 中的其他各组使用这些丰富的数据来开发用于保护客户的技术。
* IBM X-Force Exchange 是一个充满活力的全球威胁情报共享平台，旨在利用、共享并影响威胁情报，所有这一切都有 IBM X-Force 的规模和声誉的有力支撑. 用户可以搜索从机器生成的情报中提取出的各种威胁指示器，并利用人的智慧添加上下文，以便通过合作的方式进行研究并协助阻止威胁。
* IBM Security Trusteer® 产品系列提供了一个阻止整体端点网络犯罪的平台，以协助保护组织免遭金融欺诈和数据泄露。 数以百计的组织和成百上千万的终端用户依靠这些来自于 IBM Security 的产品来保护其 Web 应用程序、电脑和移动设备免遭网上威胁（例如，高级恶意软件和网络钓鱼攻击）。
* IBM X-Force 内容安全小组通过爬网、独立探索以及 IBM Managed Security Services 提供的源等方式，独立搜寻 Web 并对其进行分类。
* IBM Managed Security Services 负责监视与端点、服务器（包括 Web 服务器）和一般网络基础架构有关的攻击。 该小组会追踪通过 Web 以及其他媒介（例如，电子邮件和即时消息）产生的攻击。
* IBM Professional Security Services 交付对整个企业的安全评估、设计和部署服务，以协助建立有效的信息安全解决方案。
* IBM QRadar® Security Intelligence Platform 为安全情报和事件管理 (SIEM)、日志管理、配置管理、漏洞评估和异常状况检测提供了集成解决方案。 它提供了一个统一的仪表板，并可以实时洞察所有人员、数据、应用程序和基础架构的安全及合规性风险。
* IBM Security QRadar Incident Forensics 旨在协助企业安全小组查看网络活动，并清楚地了解用户行动。 它可以为元数据和数据包捕获中的负载内容 (PCAP) 文件设置索引，以便完整重建会话、建立数字压缩、突出显示可疑内容，并使借助于可见性来进行的搜索驱动数据探索更加容易。 QRadar Incident Forensics 可轻松与 QRadar Security Intelligence Platform 集成，并且可使用 QRadar 单一控制台管理界面进行访问。
* IBM Security AppScan® 可通过识别漏洞、利用智能修复建议生成报告以协助修正等方式，帮助组织评估 Web 和移动应用程序的安全，强化应用程序安全程序管理并实现合规性。 IBM Hosted Application Security Management 服务是基于云的解决方案，用于在生产前环境和生产环境中使用 AppScan 动态测试 Web 应用程序。
* IBM Security 身份和访问管理解决方案通过在当今的多边环境中保护并监视用户的访问权，来协助强化合规性并降低风险。 这些解决方案通过控制基于上下文的访问权、强制执行安全策略和管控业务驱动的身份，来协助保护有价值的数据和应用程序的安全。

**作者名单**

“IBM X-Force 威胁情报季度报告”的创作是整个 IBM 精诚合作的结果。 我们谨对以下人员在此报告的出版过程中所给予的悉心帮助和所做出的贡献致以深切的谢意。

**更多信息**

有关 IBM X-Force 的更多信息，请访问：

[**ibm.com**/security/xforce/](http://www.ibm.com/security/xforce/)

|  |  |
| --- | --- |
| **作者名单** | **职务** |
| Ben Wuest | 高级技术组成员，IBM Security Intelligence |
| Doug Franklin | 研究技术专家，IBM X-Force Advanced Research |
| Leslie Horacek | 经理，IBM X-Force Threat Response |
| Michael Campbell | 高级安全专家，IBM Security Systems Sales Enablement |
| Pamela Cobb | 全球细分市场经理，IBM X-Force and Threat Portfolio |
| Ralf Iffert | 经理，IBM X-Force Content Security |
| Robin Cohan | 产品经理，IBM Security Identity Management |
| Roger J. Hellman | 全球细分市场经理，IBM Security Intelligence |
| Russell Couturier | 首席技术官，IBM Network Forensics |
| Tim Kroupa | 调查主管，IBM Emergency Response Services |
| Veronica A. Shelley | 全球细分市场经理，IBM Identity and Access Management |

1. “IBM Security 服务 2015 网络安全情报索引”  
   [http://www-935.ibm.com/services/us/en/it-services/security-](http://www-935.ibm.com/services/us/en/it-services/security-services/index.html?lnk=sec_home) [services/index.html?lnk=sec\_home](http://www-935.ibm.com/services/us/en/it-services/security-services/index.html?lnk=sec_home)
2. Sean Michael Kerner 于 2014 年 6 月 16 日发布于 eWEEK 上的“AT&T 内部数据泄露比外部黑客入侵更加危险”。  
   [http://www.eweek.com/mobile/att-insider-data-breach-more-](http://www.eweek.com/mobile/att-insider-data-breach-more-dangerous-than-external-hacking.html) [dangerous-than-external-hacking.html](http://www.eweek.com/mobile/att-insider-data-breach-more-dangerous-than-external-hacking.html)
3. Darlene Storm 于 2013 年 1 月 8 日发布于《电脑世界》上的“通过黑客入侵的 VoIP 电话进行远程监听：思科正在研究窃听补丁”。  
   [http://www.computerworld.com/article/2474060/cybercrime-](http://www.computerworld.com/article/2474060/cybercrime-hacking/remotely-listen-in-via-hacked-voip-phones--cisco-working-on-eavesdropping-patch.html) [hacking/remotely-listen-in-via-hacked-voip-phones--cisco-working-](http://www.computerworld.com/article/2474060/cybercrime-hacking/remotely-listen-in-via-hacked-voip-phones--cisco-working-on-eavesdropping-patch.html) [on-eavesdropping-patch.html](http://www.computerworld.com/article/2474060/cybercrime-hacking/remotely-listen-in-via-hacked-voip-phones--cisco-working-on-eavesdropping-patch.html)
4. Chris Poulin 于 2014 年 1 月 31 日发布于“IBM Security 情报博客”上的“零售商需要从塔吉特 (Target) 数据泄露事件中学习什么来防止遭受类似的攻击”。  
   [http://securityintelligence.com/target-breach-protect-against-](http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.VUtHXPmqjRY) [similar-attacks-retailers/#.VUtHXPmqjRY](http://securityintelligence.com/target-breach-protect-against-similar-attacks-retailers/#.VUtHXPmqjRY)
5. Adam Greenberg 于 2014 年 11 月 7 日发布于《SC 杂志》上的“家得宝宣布数据泄露事件中有 53M 电子邮件地址被盗”。  
   [http://www.scmagazine.com/home-depot-announces-53m-email-](http://www.scmagazine.com/home-depot-announces-53m-email-addresses-stolen-in-breach/article/382144/) [addresses-stolen-in-breach/article/382144/](http://www.scmagazine.com/home-depot-announces-53m-email-addresses-stolen-in-breach/article/382144/)

© Copyright IBM Corporation 2015

IBM Security

Route 100

Somers, NY 10589

创作于美利坚合众国

2015 年 6 月

IBM、IBM 徽标、ibm.com、AppScan、QRadar、Trusteer 和 X-Force 是国际商业机器公司在全球许多管辖区域注册的商标。 其他产品和服务名称可能是 IBM 或其他公司的商标。 IBM 商标的当前列表可以在 Web 上的“版权与商标信息”中获取，网址为：[**ibm.com**/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml)

Linux 是 Linus Torvalds 在美国和/或其他国家或地区的注册商标。

Microsoft 和 Windows 是 Microsoft Corporation 在美国和/或其他国家或地区的商标。 Java 和所有基于 Java 的商标和徽标是 Oracle 和/或其分公司的商标或注册商标。

本文档的当前更新日期为最初发布日期，IBM 可随时进行更改。 并非所有产品在每个有 IBM 业务的国家或地区中都提供。

本文档中的信息“按现状”提供，不提供任何明示或暗含的保证，包括但不限于有关适销性、适用于某种特定用途的任何保证，以及有关非侵权的任何保证或条件。 IBM 产品根据提供该产品所依据的协议的条款和条件进行担保。

客户有责任确保其遵守适用于自身的法律和法规。 IBM 不提供法律意见，也不陈述或保证其服务或产品确保遵守法律或法规要求。 关于 IBM 未来方向和意向的声明都可随时更改或收回，而不另行通知，它们仅仅表示了目标和意愿而已。

优秀安全做法的声明： IT 系统安全包括：通过阻止、检测和响应来自您的企业内部和外部的不适当访问，保护系统和信息。 不适当的访问可能会导致信息更改、破坏、盗用或误用，也可能会导致系统损坏或误用，包括用于攻击其他系统。 不应将任何 IT 系统或产品视为完全安全，也没有任何一种产品、服务或安全措施可以完全有效地防止不适当的使用或访问。 IBM 系统、产品和服务设计为合法的全面安全方法的一部分，这将必然会涉及到其他的操作程序，并且可能要求其他系统、产品或服务是最有效的。 IBM 不保证任何系统、产品或服务不会遭受来自任何一方的恶意或非法控制，也不保证您的企业不会遭受来自任何一方的恶意或非法控制。

请回收

WGL03076-USEN-00